

**Mišljenje Europskog gospodarskog i socijalnog odbora o:****Prijedlogu uredbe Europskog parlamenta i Vijeća o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014 i (EU) br. 909/2014***(COM(2020) 595 final – 2020/0266 (COD))***Prijedlogu direktive Europskog parlamenta i Vijeća o izmjeni direktiva 2006/43/EZ, 2009/65/EZ, 2009/138/EZ, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 i (EU) 2016/2341***(COM(2020) 596 final – 2020/0268 (COD))**(2021/C 155/06)***Izvjestitelj: Antonio GARCÍA DEL RIEGO**

Zahtjev za savjetovanje:	Europski parlament, 17.12.2020. Vijeće Europske unije, 22.12.2020.
Pravni temelj:	članak 53. stavak 1., članak 114. stavak 1. i članak 304. UFEU-a
Nadležna stručna skupina:	Stručna skupina za ekonomsku i monetarnu uniju te ekonomsku i socijalnu koheziju
Datum usvajanja u Stručnoj skupini:	12.2.2021.
Datum usvajanja na plenarnom zasjedanju:	24.2.2021.
Plenarno zasjedanje br.:	558
Rezultat glasanja (za/protiv/suzdržani):	243/1/4

**1. Zaključci i preporuke**

1.1. EGSO pozdravlja prijedlog digitalne operativne otpornosti (DORA) koji je podnijela Europska komisija jer mu je cilj pružiti pravnu jasnoću u pogledu odredbi za IKT rizik, smanjiti regulatornu složenost, uspostaviti zajednički skup standarda za ublažavanje IKT rizika i omogućiti usklađeni nadzorni pristup, istodobno pružajući i pravnu sigurnost te nužne zaštitne mjere za financijska poduzeća i pružatelje usluga u području IKT-a. DORA jača otpornost sektora na IKT rizike, ali je i od interesa za brojne dionike, među ostalim klijente, ulagatelje i zaposlenike, te pridonosi provedbi održivog razvoja.

1.2. EGSO preporučuje poboljšanje učinkovitosti DORA-e s pomoću sljedećih koraka:

1.2.1. Uključivanjem u okvir DORA-e svakog pružatelja osnovnih financijskih usluga koji razvija financijske aktivnosti i isključivanjem upotrebe IKT usluga za funkcije koje nisu ključne.

1.2.2. Osiguravanjem dosljednosti u definiciji i području primjene između DORA-e i zahtjeva utvrđenih u postojećim smjernicama koje su izdala europska nadzorna tijela.

1.2.3. U pogledu upravljanja IKT-om, davanjem prednosti okviru usmjerenom na pristup utemeljen na načelima i rizicima koji olakšava provedbu kontrola koje su otporne na promjene u budućnosti, fleksibilne i proporcionalne rizicima.

1.2.4. U pogledu incidenata povezanih s IKT-om, potpunim usklađivanjem s kompletnom alatima Odbora za financijsku stabilnost za odgovor na kiberincidente i oporavak od njih.

1.2.5. U pogledu testiranja digitalne operativne otpornosti, naglašavanjem opsega financijske institucije, ali i složenosti i ključne prirode usluge; izbjegavanjem obvezne eksternalizacije koju provodi ograničen broj vanjskih provoditelja testiranja te uzajamno priznavanje rezultata testiranja.

1.2.6. Objedinjavanjem zahtjeva za eksternalizaciju u jedinstveni pravilnik kako bi se osigurala pravna sigurnost svih sudionika na tržištu i na pouzdan način ispunila očekivanja nadzora.

1.2.7. Potpunim provođenjem preporuka glavnih nadzornih tijela i jasnim skupom uloga i odgovornosti za različita nadležna tijela uključena u nadzor trećih strana pružatelja ključnih usluga.

1.2.8. Osiguravanjem pristupa eksternaliziranim uslugama koje se smatraju ključnima za treće strane pružatelje usluga sa sjedištem u trećim zemljama kako bi se izbjeglo ograničavanje ugovorne slobode poduzeća i mogućnost pristupa uslugama pružatelja usluga velike dodane vrijednosti.

1.2.9. Uključivanjem proporcionalnosti u režim sankcioniranja kako bi se izbjegle nepoticajne mjere za pružatelje usluga u području IKT-a kako bi služili financijskim subjektima u EU-u i kako bi se odmaklo od trenutne povezanosti sa svjetskim prometom.

1.2.10. Osiguravanjem jasnoće u pogledu sposobnosti poduzeća da razmjenjuju informacije o kiberprijetnjama, osiguravajući da se takvi planovi uspostave dobrovoljno i da prijedlog DORA sadržava izričitu odredbu kojom se omogućava razmjena osobnih informacija.

1.2.11. Moglo bi se razmotriti povećanje pragova za izuzeće koji su u prijedlogu utvrđeni za mikropoduzeća i mala poduzeća, kao što su definirana u članku 2. stavku 2. Priloga I. Preporuci Komisije 2003/361/EZ <sup>(1)</sup>: poduzeća s manje od 50 zaposlenih i čiji godišnji promet i/ili ukupna godišnja bilanca iznosi najviše 10 milijuna EUR, i smanjenje broja zahtjeva primjenjivih na MSP-ove razmjerno profilu digitalne rizičnosti predmetnog subjekta.

1.3. EGSO podupire osnaživanje glavnih nadzornih tijela za izvršavanje postupaka revizije i inspekcije trećih strana pružatelja ključnih usluga jer bi glavna nadzorna tijela stekla bolje razumijevanje rizika koje treće strane pružatelji ključnih usluga mogu predstavljati, a to bi moglo pomoći u pojednostavljenju postupaka eksternalizacije banaka.

## 2. Kontekst

2.1. Europski potrošači i poduzeća sve se više oslanjaju na digitalne financijske usluge, što je usko povezano sa sudionicima na tržištu koji primjenjuju sve više inovativnih rješenja temeljenih na novim tehnologijama. Digitalna transformacija ključna je za europski oporavak te za stvaranje održivog i otpornog europskog gospodarstva.

2.2. U skladu s prioritetima Europske komisije da se osigura spremnost Europe za digitalno doba i da se izgradi gospodarstvo spremno za budućnost koje je u interesu građana, Komisija je predstavila **paket o digitalnim financijama**. U tom se paketu navode mjere za daljnje omogućavanje i podupiranje potencijala digitalnog financiranja u smislu inovacija i tržišnog natjecanja uz istodobno ublažavanje rizika koji iz njih proizlaze.

2.3. Osim prijedloga o digitalnoj operativnoj otpornosti, paket o digitalnim financijama obuhvaća novu strategiju o digitalnim financijama za financijski sektor EU-a <sup>(2)</sup> i prijedlog uredbe o tržištima kriptoinovine te prijedlog uredbe o pilot-režimu za tržišne infrastrukture koje se temelje na tehnologiji decentraliziranog vođenja evidencije transakcija (DLT) <sup>(3)</sup>.

<sup>(1)</sup> SL L 124, 20.5.2003., str. 36.

<sup>(2)</sup> Vidjeti mišljenje EGSO-a ECO/534 – Strategija za digitalne financije za EU (vidjeti stranicu 27 ovoga Službenog lista).

<sup>(3)</sup> Vidjeti mišljenje EGSO-a ECO/535 – Kriptoinovina i tehnologija decentraliziranog vođenja evidencije transakcija (vidjeti stranicu 31 ovoga Službenog lista).

2.4. **Digitalna operativna otpornost** znači sposobnost poduzeća da izdrže sve vrste poremećaja i prijetnji povezanih s informacijskim i komunikacijskim tehnologijama (IKT). Sve veća ovisnost financijskog sektora o softveru i digitalnim procesima znači da su rizici povezani s IKT-om neodvojivo povezani s financijama. Financijska poduzeća postala su meta kibernetičkih napada koji uzrokuju ozbiljnu financijsku štetu i štetu za ugled potrošača i poduzeća. Te je rizike potrebno dobro razumjeti i njima upravljati, posebno u stresnim razdobljima.

2.5. Iako su reforme koje su uslijedile nakon financijske krize 2008. ojačale otpornost financijskog sektora EU-a, rizici povezani s IKT-om rješavali su se samo neizravno. Nedostatak sveobuhvatnog regulatornog okvira na europskoj razini u pogledu digitalne operativne otpornosti doveo je do oslanjanja na nacionalne regulatorne inicijative. Međutim, to ima ograničene prekogranične učinke i dovelo je do fragmentacije jedinstvenog tržišta, čime se potkopava stabilnost i integritet financijskog sektora EU-a. U tom kontekstu Komisija predlaže stvaranje sveobuhvatnog okvira o digitalnoj operativnoj otpornosti za financijske subjekte EU-a.

2.6. Cilj je **zakonodavnog prijedloga o digitalnoj operativnoj otpornosti (DORA)** <sup>(4)</sup> poboljšati i racionalizirati način na koji financijski subjekti upravljaju rizicima povezanim s IKT-om, uspostaviti temeljito testiranje otpornosti sustava IKT-a, poticati razmjenu informacija i povećati svijest nadzornih tijela o kibernetičkim i incidentima povezanim s IKT-om s kojima se suočavaju financijski subjekti te ovlastiti financijska nadzorna tijela da prate rizike koji proizlaze iz ovisnosti financijskih subjekata o trećim stranama pružateljima IKT usluga. Svrha je prijedloga i uspostava dosljednog mehanizma za izvješćivanje o incidentima koji bi mogao pridonijeti smanjenju administrativnog opterećenja za financijske subjekte i jačanju učinkovitosti nadzora.

2.7. Komisija je predstavila i prijedlog direktive <sup>(5)</sup> jer je potrebno utvrditi privremeno izuzeće za multilateralne trgovinske platforme te izmijeniti ili pojasniti određene odredbe u postojećim direktivama EU-a o financijskim uslugama kako bi se postigli ciljevi prijedloga o digitalnoj operativnoj otpornosti.

2.8. Tržište IKT-a, koje se smatra jednom od najvećih industrija na svijetu i čija je vrijednost 2019. procijenjena na više od 5 bilijuna USD, do 2022. vrijedit će više od 6 bilijuna USD. Stalan rast služi kao podsjetnik na sve veću rasprostranjenost i važnost tehnologije u današnjem društvu. **Financijski sektor najveći je korisnik IKT-a na svijetu, uz otprilike 20 % svih ukupnih troškova povezanih s IKT-om**, u skladu s procjenom učinka iz zakonodavnog prijedloga.

2.9. **Pandemija bolesti COVID-19 pokrenula je širenje digitalnih financijskih usluga**, dok su mreže poslovnica financijskih institucija i dalje nedovoljno iskorištene. To će potaknuti ulaganja u digitalne samoposlužne alate, aplikacije za otvorene financije i usluge s dodanom vrijednošću. Općenito, trenutačna situacija prisilit će financijske institucije da više ulažu u informatičku infrastrukturu, daju prednost migraciji ključnog opterećenja i ažuriraju postojeće aplikacije. Europski financijski sektor već prolazi kroz veliku digitalnu transformaciju, a njegova sposobnost da se natječe na globalnoj razini uvelike će ovisiti o sposobnosti europskih institucija da iskoriste najnaprednije tehnologije.

### 3. Opće napomene

3.1. **EGSO pozdravlja prijedlog digitalne i operativne otpornosti (DORA) koji je podnijela Europska komisija** kojim se rješavaju mnogi zahtjevi zabilježeni u financijskom sektoru, a čiji je cilj pružiti pravnu jasnoću u pogledu odredbi za IKT rizik, smanjiti regulatornu složenost i ublažiti administrativno opterećenje koje proizlazi iz različitih pravila koja se primjenjuju na financijske subjekte u cijelom EU-u. DORA jača otpornost sektora na IKT rizike, ali je i od interesa za nekoliko dionika, među ostalim klijente, ulagatelje i zaposlenike, te pridonosi provedbi održivog razvoja.

3.2. EGSO smatra da je DORA važan korak ka uspostavljanju zajedničkog skupa normi za ublažavanje IKT rizika i omogućavanje usklađenog pristupa nadzora, no potreban je oprez kako bi se izbjegle dodatne prepreke koje bi mogle spriječiti financijske institucije EU-a da budu dio globalnog inovacijskog postupka.

<sup>(4)</sup> COM(2020) 595 final.

<sup>(5)</sup> COM(2020) 596 final.

3.3. EGSO smatra da je sveobuhvatan cilj nadležnih tijela EU-a postići proporcionalan režim utemeljen na rizicima kojim se nadzornim tijelima pružaju alati za rješavanje njihovih razloga za zabrinutost, a da se istodobno pružaju pravna sigurnost i nužne zaštitne mjere za financijska poduzeća i pružatelje usluga u području IKT-a.

#### 4. Posebne napomene

##### 4.1. Područje primjene i pitanja regulatornog preklapanja

###### 4.1.1. Uključivanje dodatnih relevantnih sudionika financijskog tržišta

Iako EGSO prepoznaje i pozdravlja širok opseg sudionika financijskog tržišta na koje se odnosi predloženo zakonodavstvo kojim će se osigurati dosljedna primjena njegovih zahtjeva diljem financijskog sektora EU-a, preporučujemo da tvorcima politika EU-a uključe financijske sudionike koji se ne smatraju dijelom područja primjene tog predloženog zakonodavstva – kao što su pružatelji hipotekarnih i potrošačkih kredita – do primjerene razine utvrđene na temelju rizika koji bi mogli predstavljati za sustav. Svaki pružatelj financijskih usluga koji razvija iste djelatnosti i preuzima iste rizike trebao bi biti obuhvaćen istim pravilima i nadzorom kako bi se zajamčio isti minimalni okvir za digitalnu otpornost kojim se štite potrošači i financijska stabilnost.

###### 4.1.2. Dosljednost na međunarodnoj razini, razini EU-a i s postojećim propisima

Od presudne je važnosti osigurati jasnoću poduzećima, posebice onima s prekograničnim poslovanjem, osiguravajući da definicije i pojmovi budu dosljedni i izbjegavajući udvostručavanja, preklapanja i različita tumačenja načina na koje se slična regulatorna očekivanja mogu ispuniti u različitim jurisdikcijama. EGSO preporučuje da tvorcima politika EU-a izmijene definiciju operativne otpornosti kako bi bila u skladu s definicijom Bazelskog odbora za nadzor banaka (BCBS) <sup>(6)</sup> i kako bi se osiguralo da to bude vodeći sustav koji se primjenjuje na financijske institucije EU-a kako bi se izbjegao rizik od proturječnosti s drugima. Osim toga, mnoga načela i zahtjevi utvrđeni u DORA-i već su definirani u postojećim smjernicama o eksternalizaciji <sup>(7)</sup>. Zahtjevi za upravljanje IKT rizicima i sigurnosnim rizicima isto su tako već definirani u smjernicama EBA-e. Bit će od presudne važnosti osigurati dosljednost u definiciji i području primjene između DORA-e i zahtjeva utvrđenih u postojećim smjernicama kako bi se postigla usklađenost regulatornih zahtjeva EU-a.

4.1.3. Isto tako EGSO preporučuje da EK osigura da tekuće preispitivanje Direktive o sigurnosti mrežnih i informacijskih sustava i prijedlog o DORA-i dijele iste definicije i zahtjeve u pogledu politike izvješćivanja o sigurnosnim incidentima za financijske subjekte.

##### 4.2. Upravljanje rizicima povezanim s IKT-om

Neki elementi okvira previše su usmjereni na usklađenost, a ne na to kako poduzeća mogu predstaviti ishode u pristupu utemeljenom na načelima i rizicima. Budući da su previše preskriptivni i detaljni, postoji rizik da će s vremenom postati zastarjeli kako se područje kiberrizika i rizika povezanih s IKT-om razvija. EGSO preporučuje pristup koji je više utemeljen na načelima i rizicima i koji olakšava provedbu kontrola koje su otporne na promjene u budućnosti, fleksibilne, proporcionalne i razmjerne rizicima.

##### 4.3. Incidenti povezani s IKT-om

EGSO preporučuje potpuno usklađivanje nedavno objavljenog kompleta alata <sup>(8)</sup> Odbora za financijsku stabilnost (FSB) za odgovor na kiberincidente i oporavak od njih (CIRR), koji nudi najbolje prakse izvješćivanja o incidentima te predloženog upravljanja, klasifikacije i prijave incidenata povezanih s IKT-om predviđenih DORA-om. Postoje preklapanja koja uzrokuju regulatornu nesigurnost i povećavaju regulatorno opterećenje za poduzeća.

<sup>(6)</sup> Bazelski odbor za nadzor banaka, *Principles for operational resilience* (Načela operativne otpornosti), 6. studenoga 2020.

<sup>(7)</sup> Kao što su oni koje su izradile EBA, EIOPA te nacrt smjernica ESMA-e koje su bile u postupku savjetovanja.

<sup>(8)</sup> Odbor za financijsku stabilnost, *Final Report on Effective Practices for Cyber Incident Response and Recovery* (Završno izvješće o djelotvornim praksama za odgovor na kiberincidente i oporavak od njih), 19. listopada 2020.

#### 4.4. Testiranje digitalne operativne otpornosti

4.4.1. Iako pozdravlja paneuropski režim penetracijskih testiranja vođenih prijetnjama (TLPT) u EU-u jer će povećati učinkovitost i smanjiti fragmentaciju, EGSO preporučuje da se nadležna tijela usredotoče ne samo na veličinu ili opseg financijske institucije, nego i na složenost i važnost usluge, uzimajući u obzir načelo proporcionalnosti, gdje je to primjereno, kako bi se uklonila razlika između osnovnog testiranja za sve financijske institucije i naprednijeg testiranja za važne financijske institucije te kako bi se osiguralo da klijenti manjih financijskih subjekata budu jednako zaštićeni i da se među svim financijskim subjektima uspostave jednaki uvjeti.

4.4.2. EGSO preporučuje da eksternalizacija testiranja vanjskim provoditeljima testiranja ne bude obvezna jer je broj vanjskih provoditelja testiranja ograničen. Naime, poduzeća mogu imati vlastite interne timove za testiranja koji su upoznati s okruženjem poduzeća i mogu se brzo usmjeriti na naprednije i ciljane testove.

4.4.3. Potrebno je preispitati obuhvaćenost trećih strana pružatelja IKT usluga u opseg penetracijskog testiranja vođenog prijetnjama. Činjenica da treće strane pružatelja IKT usluga mogu služiti brojnim klijentima mogla bi dovesti do znatnog udvostručavanja testiranja, što bi moglo stvoriti relevantne rizike za treće strane pružatelje IKT usluga i klijente kojima služe.

4.4.4. Nadalje, EGSO preporučuje izričito upućivanje na **uzajamno priznavanje rezultata testiranja** s obzirom na njegovu ulogu u smanjenju rizika i osiguravanju nesmetanog funkcioniranja jedinstvenog tržišta te radi izbjegavanja povećanja troškova financijskih subjekata koji posluju prekogranično.

#### 4.5. Upravljanje IKT rizikom trećih strana i nadzorni okvir za treće strane pružatelje ključnih usluga

##### 4.5.1. Osiguravanje dosljednosti s postojećim smjernicama o eksternalizaciji

EGSO pozdravlja činjenicu da se DORA-om uspostavlja zajednički regulatorni okvir za dobro upravljanje IKT rizicima trećih strana za sve sudionike financijskog tržišta u Europi. Međutim, bit će ključno osigurati potpuno usklađivanje tog zajedničkog temelja utvrđenog u ključnim načelima (članci 25., 26. i 27.) i postojećih pravila, kao što su Smjernice o eksternalizaciji europskih nadzornih tijela (odnosno, rješavanje postojeće dihotomije u području primjene između „eksternalizacije” i „usluge treće strane”<sup>(9)</sup>). Nadalje, smatramo da je ovo odlična prilika da nadležna tijela EU-a konsolidiraju zahtjeve za eksternalizaciju u jedinstvenu uredbu, s dovoljno pojedinosti kako bi se izbjegla različita tumačenja, koja bi svim sudionicima tržišta mogla pružiti pravnu sigurnost i na pouzdan način ispunila očekivanja nadzora.

##### 4.5.2. Zahtjevi primjenjivi na ključne ili važne eksternalizirane aktivnosti

Kako bi se održala usredotočenost usmjerena na rizike, kod primjene članka 25.2. uredbu potrebna je veća preciznost u pogledu načina primjene načela proporcionalnosti, navođenjem zahtjeva koji bi bili primjenjivi na ključne ili važne eksternalizirane aktivnosti i one koji bi bili primjenjivi na ostatak<sup>(10)</sup>. EGSO preporučuje da upotreba IKT usluga za funkcije koje nisu ključne ne bude obuhvaćena područjem primjene DORA-e.

##### 4.5.3. Okvir izravnog nadzora za treće strane pružatelje ključnih usluga

EGSO pozdravlja uvođenje okvira izravnog nadzora koji će financijskim tijelima omogućiti kontinuirano praćenje aktivnosti trećih strana pružatelja ključnih usluga jer ne postoji horizontalni nespecijalizirani okvir EU-a. U predloženoj uredbi nadležna tijela EU-a trebala bi prepoznati da se izloženost financijskih institucija rizicima smanjuje zbog neprekidnog praćenja njihovih aktivnosti kada se pružatelj ključnih IKT usluga podvrgne tom nadzoru. Stoga bi taj novi nadzorni okvir trebao pomoći i u pojednostavljivanju postupaka eksternalizacije banaka smanjivanjem nekih opterećenja s kojima se financijski subjekti trenutačno suočavaju, primjerice u vezi s provedbom postupaka revizije i inspekcije koji se odnose na treće strane pružatelje usluga koje se smatraju ključnima.

<sup>(9)</sup> DORA se odnosi samo na „treće strane pružatelje IKT usluga” s obzirom na ključna načela za dobro upravljanje IKT rizikom trećih strana (Poglavlje V.), dok se područje primjene Smjernica EBA-e o eksternalizaciji temelji na definiciji eksternalizacije koja podrazumijeva da se djelatnost provodi periodično ili kontinuirano (stavak 26.). U Smjernicama EBA-e utvrđen je i popis iznimaka koje se ne smatraju eksternalizacijom (stavak 28.).

<sup>(10)</sup> Ponavljamo, bit će ključno uskladiti i definiciju „ključnih ili važnih funkcija” kako u DORA-i, tako i u Smjernicama EBA-e o eksternalizaciji. Konkretno, Smjernice EBA-e definiraju čimbenike koje financijske institucije moraju razmotriti kada procjenjuju odnose li se planovi eksternalizacije na funkciju koja je ključna ili važna (članci 29., 30. i 31.).

4.5.4. EGSO podupire osnaživanje glavnih nadzornih tijela za izvršavanje postupaka revizije i inspekcije trećih strana pružatelja ključnih usluga jer bi glavna nadzorna tijela stekla bolje razumijevanje rizika koje treće strane pružatelji ključnih usluga mogu predstavljati s pomoću znanja iz prve ruke o njihovih postupcima i prostorima, umjesto da se oslanjaju na trenutačna izvješća koja pružaju nadzirane financijske institucije i inspekcije koje provode nacionalna nadležna tijela. Iako je potrebno i dalje voditi politike ublažavanja rizika financijskih subjekata i pravna obveza ostaje na njima, ako je glavno nadzorno tijelo već obavilo inspekciju i revizije, onda financijske institucije uživaju tu dodatnu razinu sigurnosti i ne moraju ih ponovno obavljati.

#### 4.5.5. Glavno nadzorno tijelo i nacionalna nadležna tijela

Kad postupak nadzora završi, preporuke glavnog nadzornog tijela popratit će nacionalna nadležna tijela koja mogu imati vlastiti pristup provedbi nalaza glavnog nadzornog tijela za određene treće strane pružatelje ključnih usluga. EGSO preporučuje potpuno pojašnjavanje uloga i odgovornosti različitih tijela kako bi se izbjegla situacija u kojoj različita tumačenja na različite načine utječu na svakog klijenta treće strane pružatelja ključnih usluga ovisno o njihovu nadležnom tijelu i kako bi se time smanjio rizik od fragmentacije. Osim toga, te bi preporuke trebale biti u potpunosti izvršive, imajući na umu trenutačnu dvosmislenost članka 37. s obzirom na njihovu obvezujuću prirodu.

#### 4.5.6. Obustava treće strane pružatelja ključnih usluga

DORA-om se nacionalna financijska regulatorna tijelima ovlašćuju da od klijenata zatraže privremeno obustavljanje ili prekid korištenja pružatelja IKT usluga dok se rizici utvrđeni u preporukama ne riješe. Zahtjevi za svaki trenutni prekid suradnje s trećom stranom pružateljem ključnih usluga zasigurno bi utjecali na postojeće ili buduće donošenje poslovnih i trgovinskih odluka (npr. odvratanje od ulaganja u EU-u) i mogli bi utjecati na financijsku stabilnost. Prije donošenja takve odluke nadležna tijela trebala bi, među ostalim čimbenicima, pažljivo razmotriti mogući negativni učinak ukidanja usluge za financijske subjekte koji se koriste tom trećom stranom pružateljem ključnih usluga <sup>(1)</sup>, postaviti jasne kriterije za takav zahtjev i razmotriti moguća rješenja.

4.5.7. Uz to, ako je u konačnici riječ o takvoj situaciji, preporučujemo da se financijski subjekti unaprijed obavijeste o tome te da im se pruži dovoljno vremena za izlazak.

## 4.6. Očuvanje globalne konkurentnosti europskih financijskih poduzeća

4.6.1. Novim se okvirom mora očuvati sposobnost europskih financijskih poduzeća da u najmanju ruku pristupe istim tehnologijama kao njihovi globalni konkurenti. Financijska poduzeća iz EU-a natječu se na globalnoj razini, a predstojeći regulatorni okvir EU-a ne bi trebao dovoditi ta poduzeća iz EU-a u nepovoljan položaj ograničavanjem njihova pristupa najnaprednijim tehnologijama, dok god pružatelji tih tehnologija ispunjavaju standarde EU-a u pogledu otpornosti i sigurnosti.

#### 4.6.2. Treće strane pružatelji usluga sa sjedištem u trećim zemljama

Uredba ne bi trebala ograničiti mogućnost eksternalizacije usluga koje se smatraju ključnima trećim stranama pružateljima usluga sa sjedištem u trećim zemljama. To bi ograničenje definitivno ograničilo ugovornu slobodu pojedinih subjekata i sposobnost europskih financijskih institucija da pristupe uslugama pružatelja usluga velike dodane vrijednosti kojih u Europi najvjerojatnije nema u dovoljnom broju. To je još relevantnije jer je predloženi nadzorni okvir ograničen na financijski sektor, čime se stvaraju nejednaki uvjeti za druge igrače koji ne podliježu ovoj uredbi, a mogao bi se i povećati rizik od koncentracije, što se DORA-om nastoji izbjeći.

---

<sup>(1)</sup> Jedan od kriterija za određivanje pružatelja IKT usluga kao pružatelja ključnih usluga bio bi stupanj zamjenjivosti treće strane pružatelja usluga, uzimajući u obzir nedostatak stvarnih alternativa ili poteškoće s djelomičnom ili potpunom migracijom usluga (članak 28.2.). Kada bi to bio slučaj, financijskim bi institucijama bilo teško prenijeti uslugu drugom pružatelju usluga. Osim toga, zahtijevanje da se izložene financijske institucije prebace na drugog pružatelja usluge naposljetku bi pridonijelo povećanoj koncentraciji na europskom tržištu, što izričito krši svrhu ove uredbe.

#### 4.6.3. Sankcije kaznene prirode na temelju globalnog prometa

DORA-om se obuhvaćaju sankcije kaznene prirode povezane sa svjetskim prometom za pružatelje IKT usluga ako ne poštuju zahtjeve financijskih nadzornih tijela EU-a. Nerazmjerna primjena tih sankcija mogla bi odvratiti globalne pružatelje IKT usluga od pružanja usluga financijskim poduzećima EU-a, što bi financijskim poduzećima EU-a de facto moglo ograničiti izbor pružatelja usluga. Osim toga, to bi treće strane pružatelje usluga koje nisu ključne moglo odvratiti od pristajanja na režim nadzora s obzirom na strah od sankcioniranja nerazmjernim kaznama i, stoga, dovelo do smanjenja konkurencije na uzlaznom tržištu. EGSO se zalaže za uvođenje razine proporcionalnosti u režim sankcija, što je ključno za izbjegavanje nepotica jnih mjera za pružatelje IKT usluga koji žele pružati usluge financijskim subjektima EU-a.

#### 4.7. O mehanizmu razmjene informacija

4.7.1. Budući da je pravodobna razmjena informacija od presudne važnosti za učinkovito utvrđivanje vektora napada te izolaciju i sprječavanje mogućih prijetnji, EGSO pozdravlja odredbu čiji je cilj omogućiti uspostavu mehanizama za razmjenu informacija o kiberprijetnjama među financijskim institucijama na dobrovoljnoj osnovi.

4.7.2. Također preporučujemo nadležnim tijelima EU-a da među uvjetima ovog prijedloga osiguraju jasnu osnovu kojom se omogućuje razmjena osobnih informacija (kao što su IP adrese) jer bi se time smanjila nesigurnost i potaknula sposobnost financijskih subjekata da povećaju svoje obrambene sposobnosti, bolje identificiraju prijetnje i smanje rizik od međusobne zaraze. Potrebno je dodatno objašnjenje zbog povjerljive/osjetljive prirode podataka.

Bruxelles, 24. veljače 2021.

*Predsjednica*  
Europskog gospodarskog i socijalnog odbora  
Christa SCHWENG

---