DELEGIRANA UREDBA KOMISIJE (EU) 2025/295

od 24. listopada 2024.

o dopuni Uredbe (EU) 2022/2554 Europskog parlamenta i Vijeća u pogledu regulatornih tehničkih standarda o usklađivanju uvjeta koji omogućuju provedbu aktivnosti nadzora

(Tekst značajan za EGP)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 ([1]), a posebno njezin članak 41. stavak 2. drugi podstavak,

budući da:

(1) Okvirom za digitalnu operativnu otpornost za financijski sektor koji je uspostavljen Uredbom (EU) 2022/2554 uvodi se nadzorni okvir Unije za treće strane pružatelje usluga informacijske i komunikacijske tehnologije (IKT) u financijskom sektoru koje su imenovane kao ključne u skladu s člankom 31. te uredbe.

(2) Treća strana pružatelj IKT usluga koja odluči dobrovoljno uputiti zahtjev da je se imenuje kao ključnu trebala bi europskom nadzornom tijelu primatelju dostaviti sve potrebne informacije kako bi dokazala svoju ključnost u skladu s načelima i kriterijima utvrđenima u Uredbi (EU) 2022/2554. Stoga bi informacije koje treba navesti u dobrovoljno upućenom zahtjevu trebale biti dovoljno detaljne i potpune kako bi se omogućila jasna i potpuna procjena ključnosti na temelju članka 31. stavka 11. te uredbe. Relevantno europsko nadzorno tijelo trebalo bi odbiti svaki nepotpuni zahtjev i zatražiti informacije koje nedostaju.

(3) Pravnu identifikaciju trećih strana pružatelja IKT usluga obuhvaćenih područjem primjene ovog regulatornog tehničkog standarda trebalo bi uskladiti s identifikacijskom oznakom utvrđenom u Provedbenoj uredbi Komisije koja je donesena u skladu s člankom 28. stavkom 9. Uredbe (EU) 2022/2554.

(4) Nakon što ključnim trećim stranama pružateljima IKT usluga izda preporuke, glavno nadzorno tijelo trebalo bi pratiti postupaju li one u skladu s tim preporukama. Kako bi se omogućilo učinkovito i djelotvorno praćenje djelovanja koja su ključne treće strane pružatelji IKT usluga poduzele ili korektivnih mjera koje su provele u vezi s tim preporukama, glavno nadzorno tijelo trebalo bi moći zatražiti izvješća iz članka 35. stavka 1. točke (c) Uredbe (EU) 2022/2554, koja bi trebala imati oblik privremenih izvješća o napretku i završnih izvješća.

(5) Za potrebe procjene iz članka 42. stavka 1. Uredbe (EU) 2022/2554, u skladu s kojom glavno nadzorno tijelo mora ocijeniti je li objašnjenje ključne treće strane pružatelja IKT usluga dostatno, obavijest ključne treće strane pružatelja IKT usluga glavnom nadzornom tijelu o namjeri postupanja u skladu s primljenim preporukama trebala bi se dopuniti opisom djelovanja i mjera poduzetih za ublažavanje rizika navedenih u preporukama, zajedno s pripadajućim rokovima. Takvo objašnjenje trebalo bi biti u obliku plana za ispravljanje nedostataka.

(6) Budući da se od glavnog nadzornog tijela očekuje da ocijeni podugovorne aranžmane ključne treće strane pružatelja IKT usluga, potrebno je izraditi predložak za dostavu informacija o tim aranžmanima. U predlošku bi trebalo uzeti u obzir činjenicu da ključne treće strane pružatelji IKT usluga imaju drukčije strukture od financijskih subjekata.

([1]) SL L 333, 27.12.2022., str. 1., ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(7) Nakon što glavno nadzorno tijelo izda preporuke ključnoj trećoj strani pružatelju IKT usluga i nakon što nadležna tijela obavijeste relevantne financijske subjekte o rizicima utvrđenima u tim preporukama, glavno nadzorno tijelo trebalo bi pratiti i ocjenjivati kako ključna treća strana pružatelj IKT usluga provodi djelovanja i korektivne mjere radi usklađivanja s preporukama. Nadležna tijela trebala bi pratiti i procjenjivati u kojoj su mjeri financijski subjekti izloženi rizicima utvrđenima u tim preporukama. Kako bi očuvali jednake uvjete pri obavljanju svojih zadaća, posebno ako su rizici utvrđeni u preporukama ozbiljni i zajednički velikom broju financijskih subjekata u više država članica, i nadležna tijela i glavno nadzorno tijelo trebali bi međusobno razmjenjivati sve relevantne nalaze koji su im potrebni za obavljanje zadaća. Cilj je razmjene informacija osigurati da se u povratnim informacijama glavnog nadzornog tijela upućenih ključnoj trećoj strani pružatelju IKT usluga u vezi s njegovim mjerama i korektivnim mjerama uzme u obzir učinak na rizike financijskih subjekata te da se nadzorne aktivnosti nadležnih tijela temelje na procjeni koju provodi glavno nadzorno tijelo.

(8) Kako bi se omogućila učinkovita i djelotvorna razmjena informacija, nadležna tijela trebala bi u okviru svojih nadzornih aktivnosti procijeniti u kojoj su mjeri financijski subjekti koje nadziru izloženi rizicima utvrđenima u preporukama. Ta bi se procjena trebala provoditi razmjerno i na temelju rizika. Glavno nadzorno tijelo trebalo bi zatražiti od nadležnih tijela da podijele rezultate te procjene u određenim slučajevima kad su rizici povezani s preporukama ozbiljni i kad utječu na velik broj financijskih subjekata u više država članica. Kako bi se na najbolji način iskoristili resursi nadležnih tijela, pri podnošenju zahtjeva za dostavu rezultata te procjene glavno nadzorno tijelo trebalo bi uvijek uzeti u obzir da je cilj tih zahtjeva ocijeniti provedbu djelovanja i korektivnih mjera ključnih trećih strana pružatelja IKT usluga.

(9) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća ([2]) te je on dao mišljenje 22. srpnja 2024.

(10) Ova se Uredba temelji na nacrtu regulatornih tehničkih standarda koji su europska nadzorna tijela dostavila Komisiji.

(11) Zajednički odbor europskih nadzornih tijela proveo je otvoreno javno savjetovanje o nacrtu regulatornih tehničkih standarda na kojem se temelji ova Uredba, analizirao moguće povezane troškove i koristi te zatražio mišljenje Interesne skupine za bankarstvo osnovane u skladu s člankom 37. Uredbe (EU) br. 1093/2010 Europskog parlamenta i Vijeća ([3]), Interesne skupine za osiguranje i reosiguranje i Interesne skupine za strukovno mirovinsko osiguranje osnovanih u skladu s člankom 37. Uredbe (EU) br. 1094/2010 Europskog parlamenta i Vijeća ([4]) te Interesne skupine za vrijednosne papire i tržišta kapitala osnovane u skladu s člankom 37. Uredbe (EU) br. 1095/2010 Europskog parlamenta i Vijeća ([5]),

([2]) Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([3]) Uredba (EU) br. 1093/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za bankarstvo), kojom se izmjenjuje Odluka br. 716/2009/EZ i stavlja izvan snage Odluka Komisije 2009/78/EZ (SL L 331, 15.12.2010., str. 12., ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Uredba (EU) br. 1094/2010 Europskog parlamenta i Vijeća od 24. studenog 2010. o osnivanju Europskog nadzornog tijela (Europsko nadzorno tijelo za osiguranje i strukovno mirovinsko osiguranje), o izmjeni Odluke br. 716/2009/EZ i o stavljanju izvan snage Odluke Komisije 2009/79/EZ (SL L 331, 15.12.2010., str. 48., ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Uredba (EU) br. 1095/2010 Europskog parlamenta i Vijeća od 24. studenog 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za vrijednosne papire i tržišta kapitala), izmjeni Odluke br. 716/2009/EZ i stavljanju izvan snage Odluke Komisije 2009/77/EZ (SL L 331, 15.12.2010., str. 84., ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

DONIJELA JE OVU UREDBU:

Članak 1.

Informacije koje treća strana pružatelj IKT usluga treba dostaviti u zahtjevu da je se imenuje kao ključnu

1. Treća strana pružatelj usluga informacijske i komunikacijske tehnologije (IKT) u obrazloženom, dobrovoljno upućenom zahtjevu podnesenom na temelju članka 31. stavka 11. Uredbe (EU) 2022/2554 kojim traži da je se imenuje kao ključnu na temelju članka 31. stavka 1. točke (a) Uredbe (EU) 2022/2554 dostavlja sljedeće informacije:

(a) naziv pravnog subjekta;

(b) identifikacijsku oznaku pravnog subjekta;

(c) ime osobe za kontakt i podaci za kontakt ključne treće strane pružatelja IKT usluga;

(d) zemlju u kojoj pravni subjekt ima registrirano sjedište;

(e) opis korporativne strukture, što uključuje barem informacije o njegovu matičnom društvu i drugim povezanim društvima koja pružaju IKT usluge financijskim subjektima u Uniji. Te informacije prema potrebi obuhvaćaju:

  i. nazive pravnih subjekata;

  ii. identifikacijsku oznaku pravnog subjekta;

  iii. zemlju u kojoj pravni subjekt ima registrirano sjedište;

(f) procjenu tržišnog udjela treće strane pružatelja IKT usluga u financijskom sektoru Unije i procjenu tržišnog udjela po vrsti financijskog subjekta iz članka 2. stavka 1. Uredbe (EU) 2022/2554 u godini podnošenja zahtjeva da je se imenuje kao ključnu i godini prije podnošenja tog zahtjeva;

(g) opis svake IKT usluge koja se pruža financijskim subjektima u Uniji, među ostalim:

  i. opis prirode poslovanja i vrste IKT usluga koje se pružaju financijskim subjektima;

  ii. popis funkcija financijskih subjekata koje se podupiru pruženim IKT uslugama, ako je dostupan;

  iii. informacije o tome podupiru li se IKT uslugama koje se pružaju financijskim subjektima ključne ili važne funkcije, ako su dostupne;

(h) popis financijskih subjekata koji koriste IKT usluge koje pruža treća strana pružatelj IKT usluga, uključujući sljedeće informacije za svaki financijski subjekt kojem se pruža usluga, ako su dostupne:

  i. naziv pravnog subjekta;

  ii. identifikacijsku oznaka pravnog subjekta, ako je poznata trećoj strani pružatelju IKT usluga;

  iii. vrstu financijskog subjekta kako je utvrđeno u članku 2. stavku 1. Uredbe (EU) 2022/2554;

  iv. geografsku lokaciju s koje se IKT usluge pružaju predmetnom pravnom subjektu;

(i) popis ključnih trećih strana pružatelja IKT usluga uvrštenih na najnoviji dostupni popis takvih pružatelja koji su u skladu s člankom 31. stavkom 9. Uredbe (EU) 2022/2554 objavila europska nadzorna tijela koja se oslanjaju na usluge koje pruža podnositelj zahtjeva, ako je dostupan;

(j) samoprocjenu u pogledu sljedećeg:

  i. stupnja zamjenjivosti svake IKT usluge koju pruža podnositelj zahtjeva uzimajući u obzir sljedeće:

    — tržišni udio treće strane pružatelja IKT usluga u financijskom sektoru Unije,

— broj poznatih relevantnih konkurenata prema vrsti IKT usluga ili skupini IKT usluga,

— opis posebnosti povezanih s ponuđenim IKT uslugama, među ostalim u vezi sa svim zaštićenim tehnologijama ili posebnim značajkama organizacije ili aktivnosti treće strane pružatelja IKT usluga;

ii. saznanja o dostupnosti alternativnih trećih strana pružatelja istih IKT usluga koje pružaju iste IKT usluge kao treća strana pružatelj IKT usluga koja podnosi zahtjev;

(k) informacije o budućoj poslovnoj strategiji u pogledu pružanja IKT usluga i infrastrukture financijskim subjektima u Uniji, uključujući sve planirane promjene u strukturi grupe ili uprave, ulazak na nova tržišta ili nove aktivnosti;

(l) podatke o podugovarateljima treće strane pružatelja IKT usluga koji su imenovani ključnim trećim stranama pružateljima IKT usluga;

(m) sve druge razloge relevantne za zahtjev treće strane pružatelja IKT usluga da je se imenuje kao ključnu.

2. Ako je treća strana pružatelj IKT usluga dio grupe, informacije iz stavka 1. dostavljaju se u odnosu na IKT usluge koje pruža grupa kao cjelina.

Članak 2.

Sadržaj, struktura i format informacija koje trebaju dostaviti, objaviti ili o kojima trebaju izvijestiti ključne treće strane pružatelji IKT usluga

1. Ključne treće strane pružatelji IKT usluga glavnom nadzornom tijelu na njegov zahtjev dostavljaju sve informacije koje su glavnom nadzornom tijelu potrebne za obavljanje njegovih nadzornih dužnosti u skladu sa zahtjevima iz Uredbe (EU) 2022/2554.

2. Informacije iz stavka 1. uključuju, među ostalim, sljedeće:

(a) informacije o aranžmanima i preslike ugovornih dokumenata između:

i. ključne treće strane pružatelja IKT usluga i financijskih subjekata iz članka 2. stavka 1. Uredbe (EU) 2022/2554;

ii. ključne treće strane pružatelja IKT usluga i njezinih podugovaratelja kako bi se obuhvatio tehnološki vrijednosni lanac IKT usluga koje se pružaju financijskim subjektima u Uniji;

(b) informacije o organizacijskoj strukturi i strukturi grupe ključne treće strane pružatelja IKT usluga, uključujući identifikaciju svih subjekata koji pripadaju istoj grupi, koja izravno ili neizravno pruža IKT usluge financijskim subjektima u Uniji;

(c) informacije o glavnim dioničarima, uključujući njihovu strukturu i zemljopisnu raširenost, bilo kojeg od sljedećeg:

i. subjekata koji samostalno ili zajedno sa svojim povezanim subjektima drže 25 % ili više kapitala ili glasačkih prava u ključnoj trećoj strani pružatelju IKT usluga;

ii. subjekata koji imaju pravo imenovati ili smijeniti većinu članova upravnog, upravljačkog ili nadzornog tijela ključne treće strane pružatelja IKT usluga;

iii. subjekata koji kontroliraju, na temelju sporazuma, većinu glasačkih prava dioničara ili članova ključne treće strane pružatelja IKT usluga;

(d) informacije o tržišnom udjelu ključne treće strane pružatelja IKT usluga prema vrsti usluga na relevantnim tržištima na kojima posluje;

(e) informacije o mehanizmima unutarnjeg upravljanja ključne treće strane pružatelja IKT usluga, uključujući strukturu s linijama upravljačke odgovornosti i pravilima o odgovornosti;

(f) zapisnike sa sastanaka upravljačkog tijela ključne treće strane pružatelje IKT usluga i svih drugih internih relevantnih odbora, koji se na bilo koji način odnose na aktivnosti i rizike povezane s IKT uslugama trećih strana kojima se podupiru funkcije financijskih subjekata u Uniji;

(g) informacije o sigurnosti IKT-a ključne treće strane pružatelja IKT usluga, uključujući relevantne strategije, ciljeve, politike, postupke, protokole, procese, kontrolne mjere za zaštitu osjetljivih podataka, kontrole pristupa, prakse šifriranja, planove odgovora na incidente i informacije o usklađenosti sa svim relevantnim propisima te, prema potrebi, nacionalnim i međunarodnim normama;

(h) informacije o tehničkim i organizacijskim mjerama za osiguravanje zaštite i povjerljivosti podataka, uključujući osobne i neosobne podatke, provedenim kontrolnim mjerama za zaštitu osjetljivih podataka, kontrolama pristupa, praksama šifriranja i planu za odgovor na povredu podataka; kad je riječ o obradi osobnih podataka, treća strana pružatelj IKT usluga podliježe zakonima trećih zemalja, uključujući zahtjev vlada trećih zemalja za pristup, popis zemalja i primjenjive zakone;

(i) informacije o mehanizmima za prenosivost podataka, prenosivost aplikacija i interoperabilnost koje ključna treća strana pružatelj IKT usluga nudi financijskim subjektima u Uniji;

(j) informacije o lokaciji podatkovnih centara i proizvodnih centara za IKT koji se upotrebljavaju za potrebe pružanja usluga financijskim subjektima, uključujući popis svih relevantnih poslovnih prostora i objekata ključne treće strane pružatelja IKT usluga, među ostalim izvan Unije;

(k) informacije o pružanju usluga ključne treće strane pružatelja IKT usluga iz trećih zemalja, uključujući informacije o relevantnim pravnim odredbama koje se primjenjuju na osobne i neosobne podatke koje obrađuje ta treća strana pružatelj IKT usluga;

(l) informacije o mjerama poduzetima za nošenje s rizicima koji proizlaze iz pružanja IKT usluga ključne treće strane pružatelja IKT usluga i njezinih podugovaratelja iz trećih zemalja;

(m) informacije o okviru za upravljanje rizicima i okviru za upravljanje incidentima, koje obuhvaćaju politike, postupke, alate, mehanizme i aranžmane upravljanja ključne treće strane pružatelja IKT usluga i njezinih podugovaratelja, među ostalim popis i opis značajnih incidenata s izravnim ili neizravnim učinkom na financijske subjekte u Uniji, te relevantne pojedinosti za utvrđivanje važnosti incidenta za financijske subjekte i procjenu mogućih prekograničnih učinaka;

(n) informacije o okviru za upravljanje promjenama, koje uključuju politike, postupke i kontrole ključne treće strane pružatelja IKT usluga i njezinih podugovaratelja;

(o) informacije o općem okviru za odgovor i oporavak ključne treće strane pružatelja IKT usluga, uključujući planove kontinuiteta poslovanja i povezane aranžmane i postupke, politiku životnog ciklusa razvoja softvera, planove odgovora i oporavka i povezane aranžmane i postupke te aranžmane i postupke za izradu sigurnosnih kopija;

(p) informacije o praćenju uspješnosti, sigurnosti i incidenata te informacije o mehanizmima izvješćivanja o uspješnosti usluga, incidentima i usklađenosti s dogovorenim sporazumima o razini usluga i ciljevima u pogledu razine usluga ili sličnim aranžmanima između ključnih trećih strana pružatelja IKT usluga i financijskih subjekata u Uniji;

(q) informacije o okviru upravljanja trećim stranama pružateljima IKT usluga ključne treće strane pružatelja IKT usluga, uključujući strategije, politike, postupke, procese i kontrole te pojedinosti o dubinskoj analizi i procjeni rizika koju ključna treća strana pružatelj IKT usluga provodi nad svojim podugovarateljima prije sklapanja sporazuma s njima te radi praćenja tog odnosa što obuhvaća sve relevantne IKT rizike i rizike druge ugovorne strane;

(r) izvatke iz sustava za praćenje i skeniranje ključne treće strane pružatelja IKT usluga i njezinih podugovaratelja, koji obuhvaćaju, ali nisu ograničeni na: praćenje mreže, praćenje poslužitelja, praćenje aplikacija, praćenje sigurnosti, skeniranje ranjivosti, upravljanje zapisima, praćenje uspješnosti, upravljanje incidentima i mjerenja u odnosu na ciljeve pouzdanosti, kao što su ciljevi u pogledu razine usluga;

(s) izvatke iz bilo kojeg produkcijskog, pretprodukcijskog i ispitnog sustava ili aplikacije koje ključna treća strana pružatelj IKT usluga i njezini podugovaratelji upotrebljavaju za izravno ili neizravno pružanje usluga financijskim subjektima u Uniji;

(t) izvješća o usklađenosti i dostupna revizijska izvješća, kao i sve relevantne nalaze revizija, uključujući revizije koje provode nacionalna tijela u Uniji i izvan nje ako je sporazumima o suradnji s relevantnim tijelima predviđena takva razmjena informacija, ili certifikate koje je ishodila ključna treća strana pružatelj IKT usluga ili njezini podugovaratelji, uključujući izvješća unutarnjih i vanjskih revizora, certifikate ili ocjene usklađenosti s industrijskim normama. To uključuje informacije o svim vrstama dostupnih neovisnih testiranja otpornosti IKT sustava ključne treće strane pružatelja IKT usluga, uključujući sve vrste penetracijskog testiranja vođenog prijetnjama koje provodi treća strana pružatelj IKT usluga;

(u) informacije o svim procjenama koje je ključna treća strana pružatelj IKT usluga provela na njegov zahtjev ili u njegovo ime kojima se ocjenjuje prikladnost i integritet pojedinaca na ključnim položajima u ključnoj trećoj strani pružatelju IKT usluga;

(v) informacije o svim planovima za ispravljanje nedostataka namijenjenima provedbi preporuka u skladu s člankom 3. i relevantne povezane informacije kojima se potvrđuje provedba korektivnih mjera;

(w) informacije o dostupnim programima osposobljavanja zaposlenika i programima informiranja o sigurnosti, uključujući, prema potrebi, informacije o ulaganjima, resursima i metodama ključne treće strane pružatelja IKT usluga u osposobljavanju njegova osoblja za postupanje s osjetljivim financijskim podacima i održavanje visoke razine sigurnosti;

(x) informacije o aktivnostima ključne treće strane pružatelja IKT usluga i financijskim izvještajima, uključujući informacije o proračunu i sredstvima povezanima s IKT-om i sigurnošću.

Članak 3.

Informacije koje ključne treće strane pružatelji IKT usluga dostavljaju nakon izdavanja preporuka

1. Ključna treća strana pružatelj IKT usluga glavnom nadzornom tijelu dostavlja izvješće s planom za ispravljanje nedostataka koji se temelji na preporukama i korektivnim mjerama koje ključna treća strana pružatelj IKT usluga planira provesti kako bi ublažila rizike utvrđene u preporukama iz članka 35. stavka 1. točke (d) Uredbe (EU) 2022/2254. Izvješće se dostavlja u roku koji glavno nadzorno tijelo odredi za svaku preporuku.

2. Kako bi se omogućilo praćenje djelovanja koja je ključna treća strana pružatelj IKT usluga poduzela ili korektivnih mjera koje je provela u vezi s primljenim preporukama, ključna treća strana pružatelj IKT usluga na zahtjev glavnog nadzornog tijela s njim dijeli:

(a) privremena izvješća o napretku i pripadajuće popratne dokumente u kojima se opisuje napredak u poduzimanju djelovanja i provedbi mjera utvrđenih u izvješću koje je ključna treća strana pružatelj IKT usluga dostavila glavnom nadzornom tijelu u roku koji je ono utvrdilo;

(b) završna izvješća i pripadajuće popratne dokumente u kojima se opisuju djelovanja koja je ključna treća strana pružatelj IKT usluga poduzela ili korektivne mjere koje je provela kako bi ublažila rizike utvrđene u primljenim preporukama.

Članak 4.

Struktura i format informacija koje dostavljaju ključne treće strane pružatelji IKT usluga

1. Ključna treća strana pružatelj IKT usluga dostavlja tražene informacije glavnom nadzornom tijelu namjenskim, sigurnim elektroničkim kanalima koje je glavno nadzorno tijelo navelo u svojem zahtjevu i u obliku koji je ono utvrdilo.

2. Pri dostavljanju informacija glavnom nadzornom tijelu ključne treće strane pružatelji IKT usluga dužne su:

(a) pratiti strukturu koju je glavno nadzorno tijelo navelo u zahtjevu za informacije;

(b) jasno locirati relevantne informacije u podnesenoj dokumentaciji.

3. Informacije koje ključna treća strana pružatelj IKT usluga dostavi ili otkrije glavnom nadzornom tijelu ili o kojima izvijesti glavno nadzorno tijelo moraju biti na jeziku koji je uobičajen u području međunarodnih financija.

Članak 5.

Predložak za dostavljanje informacija o podugovornim aranžmanima

Ključna treća strana pružatelj IKT usluga koja je dužna podijeliti informacije o podugovornim aranžmanima dostavlja te informacije glavnom nadzornom tijelu u predlošku iz Priloga.

Članak 6.

Procjena rizika navedenih u preporukama glavnog nadzornog tijela koju provode nadležna tijela

1. U okviru nadzora financijskih subjekata nadležno tijelo u skladu s načelom proporcionalnosti procjenjuje učinak koji na financijske subjekte imaju mjere koje je ključna treća strana pružatelj IKT usluga poduzela na temelju preporuka glavnog nadzornog tijela.

2. Pri provedbi procjene iz stavka 1. nadležno tijelo uzima u obzir sve sljedeće:

(a) primjerenost i usklađenost korektivnih mjera koje su financijski subjekti proveli kako bi ublažili rizike utvrđene u preporukama;

(b) ocjenu glavnog nadzornog tijela o postupanju ključne treće strane pružatelja IKT usluga u skladu s mjerama i djelovanjima obuhvaćenima izvješćem ako to utječe na izloženost financijskih subjekata u njezinoj nadležnosti rizicima koji su utvrđeni u preporukama;

(c) stajališta svih drugih nadležnih tijela s kojima je provedeno savjetovanje u skladu s člankom 42. stavkom 5. Uredbe (EU) 2022/2554;

(d) činjenicu smatra li glavno nadzorno tijelo da su djelovanja i korektivne mjere koje je provela ključna treća strana pružatelj IKT usluga primjerene za ublažavanje izloženosti financijskih subjekata u njezinoj nadležnosti rizicima koji su utvrđeni u preporukama.

3. Nadležno tijelo na zahtjev glavnog nadzornog tijela u razumnom roku dostavlja rezultate procjene iz stavka 1. Kad traži rezultate te procjene glavno nadzorno tijelo dužno je uzeti u obzir načelo proporcionalnosti i razmjer rizika povezanih s preporukama, uključujući prekogranične učinke tih rizika ako utječu na financijske subjekte koji posluju u nekoliko država članica.

4. Nadležno tijelo dužno je, kada je to relevantno, zatražiti od financijskih subjekata da dostave sve informacije potrebne za provedbu procjene iz stavka 1.

Članak 7.

Stupanje na snagu

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

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu 24. listopada 2024.

Za Komisiju
Predsjednica
Ursula VON DER LEYEN

PRILOG

PREDLOŽAK ZA DOSTAVU INFORMACIJA O PODUGOVORNIM ARANŽMANIMA

Kategorija informacija	Ključni elementi informacija
Opće informacije	— Naziv ključne treće strane pružatelja IKT usluga, — identifikacijska oznaka ključne treće strane pružatelja IKT usluga, — ime i prezime osobe za kontakt i podaci za kontakt ključne treće strane pružatelja IKT usluga, — datum podnošenja predloška.
Pregled podugovornih aranžmana	— Prikaz podugovornih aranžmana, uključujući kratak opis svrhe i opsega podugovornih odnosa (uključujući naznaku razine ključnosti ili važnosti podugovornih aranžmana za ključnu treću stranu pružatelja IKT usluga), — specifikacija i opis vrsta IKT usluga koje su podugovorene i njihova važnost za IKT usluge koje se pružaju financijskim subjektima, u skladu s provedbenim tehničkim standardima donesenima na temelju članka 28. stavka 9. Uredbe (EU) 2022/2554, — za potrebe navođenja vrsta IKT usluga vidjeti popis iz Priloga IV. provedbenim tehničkim standardima donesenima na temelju članka 28. stavka 9. Uredbe (EU) 2022/2554.
Informacije o podugovarateljima	— Naziv i podaci pravnog subjekta (uključujući identifikacijsku oznaku) svakog podugovaratelja, — podaci za kontakt članova osoblja odgovornih za svaki podugovorni odnos u upravljačkoj strukturi ključnih trećih strana pružatelja IKT usluga, — pregled stručnog znanja, iskustva i kvalifikacija povezanih s ugovorenim IKT uslugama za svakog podugovaratelja.
Opis usluga koje pružaju podugovaratelji	— Detaljan opis konkretnih IKT usluga koje pruža svaki podugovaratelj, — raščlamba odgovornosti i zadaća dodijeljenih podugovarateljima navođenjem pojedinosti o njihovim ulogama u pojedinim fazama IKT procesa, — informacije o razini pristupa podugovaratelja osobnim ili drugim osjetljivim podacima ili sustavima povezanima s IKT uslugama koje se pružaju financijskim subjektima, — informacije o lokacijama s kojih se pružaju usluge podugovaratelja i o mjerama poduzetima za nošenje s rizicima koji proizlaze iz usluga koje se pružaju izvan Unije.
Upravljanje i nadzor podugovaranja	— Opis ugovornog i upravljačkog okvira uspostavljenog za potrebe upravljanja podugovornim odnosima, uključujući klauzule kojima se ograničava upotreba osjetljivih podataka, — objašnjenje postupaka za odabir, angažiranje i praćenje podugovaratelja, — pregled parametara uspješnosti, ciljeva u pogledu razine usluga i sporazuma o razini usluga te ključnih pokazatelja uspješnosti koji služe za procjenu rada i praćenje pouzdanosti podugovaratelja.
Upravljanje rizicima i usklađenost	— Procjena profila rizičnosti podugovaratelja i mogućeg učinka na IKT usluge koje se pružaju financijskim subjektima, — objašnjenje mjera za ublažavanje rizika koje se provode za potrebe nošenja s rizicima povezanima s podugovaranjem, — pojedinosti o usklađenosti podugovaratelja s relevantnim propisima, među ostalim propisima o zaštiti podataka i industrijskim normama.

Kategorija informacija	Ključni elementi informacija
Planiranje kontinuiteta poslovanja i djelovanja u nepredvidivim situacijama	— Pregled planova kontinuiteta poslovanja i planova odgovora i oporavka koje su izradili podugovaratelji, — opis aranžmana za osiguranje kontinuiteta usluga u slučaju poremećaja ili raskida ugovornog aranžmana na zahtjev podugovaratelja, — učestalost testiranja planova kontinuiteta poslovanja i planova odgovora i oporavka koje provode podugovaratelji, datumi posljednjih testiranja u protekle tri godine i informacija o tome je li ključna treća strana pružatelj IKT usluga sudjelovala u tim testiranjima.
Izvješćivanje	— Opis mehanizama izvješćivanja i učestalosti izvješćivanja između ključne treće strane pružatelja IKT usluga i njezinih podugovaratelja.
Ispravljanje nedostataka i upravljanje incidentima	— Pregled postupaka za rješavanje incidenata, povreda ili neusklađenosti povezanih s podugovarateljima.
Certifikati i revizije	— Informacije o svim certifikatima, neovisnim revizijama ili ocjenama podugovaratelja kojima se potvrđuju njihove sigurnosne kontrole, standardi kvalitete ili usklađenost s propisima, — datum i učestalost revizija podugovaratelja koje provodi ključna treća strana pružatelj IKT usluga.