2024/1773

25.6.2024.

DELEGIRANA UREDBA KOMISIJE (EU) 2024/1773

od 13. ožujka 2024.

o dopuni Uredbe (EU) 2022/2554 Europskog parlamenta i Vijeća u pogledu regulatornih tehničkih standarda kojima se utvrđuje detaljan sadržaj politike o ugovornim aranžmanima u vezi s upotrebom IKT usluga kojima se podupiru ključne ili važne funkcije, a koje pružaju treće strane pružatelji IKT usluga

(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 28. stavak 10. treći podstavak,

budući da:

(1) Okvirom za digitalnu operativnu otpornost za financijski sektor uspostavljenim u Uredbi (EU) 2022/2554 zahtijeva se da financijski subjekti utvrde određena ključna načela za upravljanje IKT rizikom povezanim s trećim stranama, koja su posebno važna kad financijski subjekti angažiraju treće strane pružatelje IKT usluga kako bi poduprli svoje ključne ili važne funkcije.

(2) Financijski subjekti, kao dio svojeg okvira za upravljanje IKT rizicima, trebaju donijeti i redovito preispitivati strategiju za IKT rizik povezan s trećim stranama. U skladu s člankom 28. stavkom 2. Uredbe (EU) 2022/2554 ta strategija treba uključivati politiku o upotrebi IKT usluga kojima se podupiru ključne ili važne funkcije, a koje pružaju treće strane pružatelji IKT usluga. Primjenjuje se na pojedinačnoj i, prema potrebi, na potkonsolidiranoj i konsolidiranoj osnovi.

(3) Financijski subjekti uvelike se razlikuju po veličini, strukturi i unutarnjoj organizaciji te prirodi i složenosti njihovih aktivnosti i poslovanja. Pri izradi politike o ugovornim aranžmanima u vezi s upotrebom IKT usluga kojima se podupiru ključne ili važne funkcije, a koje pružaju treće strane pružatelji IKT usluga („politika”) potrebno je uzeti u obzir tu raznolikost kad se uvode određeni temeljni regulatorni zahtjevi koji su primjereni za sve financijske subjekte te osigurati da se ti zahtjevi primjenjuju razmjerno.

(4) Ako financijski subjekti pripadaju grupi, matično društvo koje je odgovorno za izradu konsolidiranih ili potkonsolidiranih financijskih izvještaja za grupu trebalo bi stoga osigurati dosljednu i usklađenu primjenu politike unutar grupe.

(5) U primjeni politike pružatelje IKT usluga unutar grupe, uključujući one koji su u potpunom ili zajedničkom vlasništvu financijskih subjekata unutar istog institucionalnog sustava zaštite, trebalo bi smatrati trećim stranama pružateljima IKT usluga. Rizici koje predstavljaju pružatelji IKT usluga unutar grupe mogu biti različiti, ali se na njih primjenjuju isti zahtjevi na temelju Uredbe (EU) 2022/2554. Slično tome, politika bi se trebala primjenjivati na podugovaratelje koji trećim stranama pružateljima IKT usluga pružaju IKT usluge kojima se podupiru ključne ili važne funkcije ili njihovi bitni dijelovi ako postoji lanac trećih strana pružatelja IKT usluga.

(6) Za upravljanje IKT rizikom financijskog subjekta krajnje je odgovorno upravljačko tijelo, a to se opće načelo primjenjuje i na angažiranje trećih strana pružatelja IKT usluga. Tu bi odgovornost trebalo dodatno prenijeti u kontinuirani angažman upravljačkog tijela u kontroli i praćenju upravljanja IKT rizicima, pa i u donošenju i preispitivanju politike najmanje jednom godišnje.

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

(7) Kako bi se osiguralo odgovarajuće izvješćivanje upravljačkog tijela, u politici bi trebalo jasno definirati i prepoznati unutarnje odgovornosti za odobravanje, upravljanje, kontrolu i dokumentiranje ugovornih aranžmana o upotrebi IKT usluga kojima se podupiru ključne ili važne funkcije, a koje pružaju treće strane pružatelji IKT usluga („ugovorni aranžmani”), uključujući IKT usluge koje se pružaju u okviru ugovornih aranžmana iz članka 28. stavka 1. točke (a) Uredbe (EU) 2022/2554.

(8) Kako bi se uzeli u obzir svi mogući rizici koji mogu nastati pri ugovaranju IKT usluga kojima se podupire ključna ili važna funkcija, struktura politike trebala bi slijediti sve korake glavnih faza životnog ciklusa za ugovorne aranžmane s trećim stranama pružateljima usluga.

(9) Radi ublažavanja utvrđenih rizika, u politici bi trebalo utvrditi planiranje ugovornih aranžmana, uključujući procjenu rizika, dubinsku analizu i postupak odobravanja novih ili bitnih promjena tih ugovornih aranžmana. Za potrebe upravljanja rizicima koji se mogu pojaviti prije sklapanja ugovora s trećom stranom pružateljem IKT usluga, politikom bi trebalo utvrditi primjeren i razmjeran postupak odabira i ocjenjivanja prikladnosti potencijalnih trećih strana pružatelja IKT usluga i od financijskih subjekata zahtijevati da uzmu u obzir neiscrpan popis elemenata koje bi trebale imati treće strane pružatelji IKT usluga. Popis bi trebao uključivati elemente povezane s poslovnim ugledom pružatelja usluga, njihovim financijskim, ljudskim i tehničkim resursima, informacijskom sigurnošću, organizacijskom strukturom, uključujući upravljanje rizicima, i njihovim unutarnjim kontrolama.

(10) Kako bi se osiguralo dobro upravljanje rizicima koji nastaju kad treće strane pružatelji IKT usluga pružaju IKT usluge kojima se podupiru ključne ili važne funkcije, politika bi trebala sadržavati informacije o provedbi, praćenju i upravljanju ugovornim aranžmanima, uključujući prema potrebi na konsolidiranoj i potkonsolidiranoj razini. To uključuje zahtjeve za ugovorne klauzule o uzajamnim obvezama financijskih subjekata i trećih strana pružatelja IKT usluga, koje bi trebalo utvrditi u pisanom obliku. Kako bi se osigurao učinkovit nadzor i otpornost u slučaju promjena poslovnog modela ili poslovnog okruženja, politikom bi trebalo zajamčiti prava financijskih subjekata ili imenovanih trećih strana i nadležnih tijela na inspekcijske nadzore i pristup informacijama te dodatno utvrditi izlazne strategije i postupke raskida.

(11) Ako treće strane pružatelji IKT usluga obrađuju osobne podatke, tom se politikom i ugovornim aranžmanima ne dovode u pitanje obveze na temelju Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća ([2]) i trebali bi ih dopunjavati, kao što su sklapanje pisanog ugovora u kojem se opisuje obrada osobnih podataka, zahtjev za jamčenje sigurnosti obrade osobnih podataka i utvrđivanje drugih elemenata propisanih tom uredbom.

([2]) 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., ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) Zajednički odbor europskih nadzornih tijela iz članka 54. Uredbe (EU) br. 1093/2010 Europskog parlamenta i Vijeća ([3]), članka 54. Uredbe (EU) br. 1094/2010 Europskog parlamenta i Vijeća ([4]) i članka 54. Uredbe (EU) br. 1095/2010 Europskog parlamenta i Vijeća ([5]) proveo je otvoreno javno savjetovanje o nacrtu regulatornih tehničkih standarda na kojem se temelji ova Uredba, analizirao je moguće troškove i koristi predloženih standarda te zatražio savjet Interesne skupine za bankarstvo osnovane u skladu s člankom 37. Uredbe (EU) br. 1093/2010 Europskog parlamenta i Vijeća, 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 i Interesne skupine za vrijednosne papire i tržišta kapitala osnovane u skladu s člankom 37. Uredbe (EU) br. 1095/2010,

(13) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća ([6]) te je on dao mišljenje 24. siječnja 2024.,

DONIJELA JE OVU UREDBU:

Članak 1.

Ukupni profil rizičnosti i složenost

U politici upotrebe IKT usluga kojima se podupiru ključne ili važne funkcije, a koje pružaju treće strane pružatelji IKT usluga („politika”) uzimaju se u obzir veličina i ukupni profil rizičnosti financijskog subjekta te priroda, opseg i elementi povećane ili smanjene složenosti njegovih usluga, aktivnosti i poslovanja, uključujući elemente koji se odnose na:

(a) vrstu IKT usluga uključenih u ugovorni aranžman o upotrebi IKT usluga kojima se podupiru ključne ili važne funkcije, a koje pružaju treće strane pružatelji IKT usluga („ugovorni aranžman”) između financijskog subjekta i treće strane pružatelja IKT usluga;

(b) lokaciju treće strane pružatelja IKT usluga ili lokaciju njezina matičnog društva;

(c) pruža li IKT usluge kojima se podupiru ključne ili važne funkcije treća strana pružatelj IKT usluga koja se nalazi u državi članici ili u trećoj zemlji, uzimajući u obzir i lokaciju s koje se pružaju IKT usluge i lokaciju na kojoj se podaci obrađuju i pohranjuju;

(d) prirodu podataka koji se razmjenjuju s trećom stranom pružateljem IKT usluga;

(e) je li treća strana pružatelj IKT usluga dio iste grupe kao i financijski subjekt kojem se pružaju usluge;

([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. studenoga 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).

([6]) 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).

(f) angažiranje trećih strana pružatelja IKT usluga koje su dobile odobrenje za rad, registrirane ili podliježu nadzoru nadležnog tijela u državi članici ili koje podliježu nadzornom okviru iz poglavlja V. odjeljka II. Uredbe (EU) 2022/2554 te angažiranje ostalih trećih strana pružatelja IKT usluga koje to nisu;

(g) angažiranje trećih strana pružatelja IKT usluga koje su dobile odobrenje za rad, registrirane ili podliježu nadzoru nadzornog tijela u trećoj zemlji te angažiranje ostalih trećih strana pružatelja IKT usluga;

(h) pitanje pruža li IKT usluge kojima se podupiru ključne ili važne funkcije samo jedna treća strana pružatelja IKT usluga ili mali broj takvih pružatelja usluga;

(i) prenosivost IKT usluga kojima se podupiru ključne ili važne funkcije na drugu treću stranu pružatelja IKT usluga, među ostalim zbog tehnoloških posebnosti;

(j) mogući učinak poremećaja u pružanju IKT usluga kojima se podupiru ključne ili važne funkcije na kontinuitet aktivnosti financijskog subjekta i dostupnost njegovih usluga.

Članak 2.

Primjena na razini grupe

Ako se ova Uredba primjenjuje na potkonsolidiranoj ili konsolidiranoj osnovi, matično društvo koje je odgovorno za izradu konsolidiranih ili potkonsolidiranih financijskih izvještaja za grupu osigurava da se politika dosljedno provodi u svim financijskim subjektima u okviru te grupe te da je primjerena za učinkovitu primjenu ove Uredbe na svim odgovarajućim razinama grupe.

Članak 3.

Aranžmani upravljanja

1. Upravljačko tijelo najmanje jednom godišnje preispituje politiku i prema potrebi je ažurira. Izmjene treba pravodobno i što prije unositi u politike u okviru relevantnih ugovornih aranžmana. Financijski subjekt dokumentira planirani rok za provedbu.

2. Politikom se utvrđuje metodologija za utvrđivanje ključnih ili važnih funkcija IKT usluga ili se na nju upućuje. U politici se navodi i kad tu ocjenu treba provesti i preispitati.

3. Politikom se jasno dodjeljuju unutarnje odgovornosti za odobravanje, upravljanje, kontrolu i dokumentiranje relevantnih ugovornih aranžmana te se osigurava da se u financijskom subjektu održavaju odgovarajuće vještine, iskustvo i znanje za djelotvoran nadzor relevantnih ugovornih aranžmana, uključujući IKT usluge koje se pružaju u okviru tih aranžmana.

4. Ne dovodeći u pitanje konačnu odgovornost financijskog subjekta za djelotvoran nadzor relevantnih ugovornih aranžmana, u politici se utvrđuje da treba ocijeniti ima li treća strana pružatelj IKT usluga dostatna sredstva kako bi osigurala da financijski subjekt ispunjava sve svoje pravne i regulatorne zahtjeve u pogledu IKT usluga kojima se podupiru ključne ili važne funkcije, koje on pruža.

5. Politikom se jasno utvrđuje funkcija ili član višeg rukovodstva odgovoran za praćenje relevantnih ugovornih aranžmana. Utvrđuje se i način na koji ta funkcija ili član višeg rukovodstva surađuje s kontrolnim funkcijama, osim ako je njihov dio, i uspostavljaju se linije izvješćivanja upravljačkog tijela, uključujući vrstu informacija o kojima se izvješćuje i dokumente koje treba dostaviti. Utvrđuje se i učestalost takvog izvješćivanja.

6. Politikom se osigurava da su ugovorni aranžmani u skladu sa sljedećim:

(a) okvirom za upravljanje IKT rizicima iz članka 6. Uredbe (EU) 2022/2554;

(b) politikom financijske sigurnosti iz članka 9. stavka 4. Uredbe (EU) 2022/2554;

(c) politikom kontinuiteta poslovanja u području IKT-a iz članka 11. Uredbe (EU) 2022/2554;

(d) zahtjevima u pogledu izvješćivanja o incidentima iz članka 19. Uredbe (EU) 2022/2554.

7. Politikom se utvrđuje da IKT usluge kojima se podupiru ključne ili važne funkcije koje pružaju treće strane pružatelji IKT usluga podliježu neovisnom preispitivanju i da su uključene u plan revizije.

8. U politici se izričito navodi da se ugovornim aranžmanima:

(a) financijski subjekt i njegovo upravljačko tijelo ne oslobađaju od regulatornih obveza i odgovornosti prema klijentima;

(b) ne smije sprečavati djelotvoran nadzor financijskog subjekta niti kršiti nadzorna ograničenja usluga i aktivnosti;

(c) od trećih strana pružatelja IKT usluga zahtijeva suradnja s nadležnim tijelima;

(d) od financijskog subjekta, njegovih revizora i nadležnih tijela zahtijeva omogućavanje djelotvornog pristupa podacima i prostorijama za upotrebu IKT usluga kojima se podupiru ključne ili važne funkcije.

Članak 4.

Glavne faze životnog ciklusa ugovornih aranžmana

Politikom se utvrđuju zahtjevi, uključujući pravila, odgovornosti i procese, za svaku glavnu fazu životnog ciklusa ugovornog aranžmana, koji obuhvaćaju barem sljedeće:

(a) odgovornosti upravljačkog tijela, uključujući prema potrebi njegovo sudjelovanje u postupku donošenja odluka o upotrebi IKT usluga kojima se podupiru ključne ili važne funkcije trećih strana pružatelja IKT usluga;

(b) planiranje ugovornih aranžmana, uključujući procjenu rizika, dubinsku analizu kako je utvrđena u člancima 5. i 6. i postupak odobravanja novih ili bitnih promjena ugovornih aranžmana kako je utvrđeno u članku 8. stavku 4.;

(c) sudjelovanje poslovnih jedinica, unutarnjih kontrola i drugih jedinica relevantnih za ugovorne aranžmane;

(d) provedbu, praćenje i upravljanje ugovornim aranžmanima iz članaka 7., 8. i 9., uključujući prema potrebi na konsolidiranoj i potkonsolidiranoj razini;

(e) dokumentiranje i vođenje evidencije, uzimajući u obzir zahtjeve u pogledu registra informacija utvrđene u članku 28. stavku 3. Uredbe (EU) 2022/2554;

(f) izlazne strategije i postupke prekida kako su utvrđeni u članku 10.

Članak 5.

Ex ante procjena rizika

1. Politikom se utvrđuje da se prije sklapanja ugovora definiraju poslovne potrebe financijskog subjekta.

2. Politikom se utvrđuje da se procjena rizika provodi na razini financijskog subjekta i, prema potrebi, na konsolidiranoj i potkonsolidiranoj razini prije sklapanja ugovornog aranžmana.

U procjeni rizika uzimaju se u obzir svi relevantni zahtjevi utvrđeni u Uredbi (EU) 2022/2554 i primjenjivi sektorski propisi Unije. Posebno se uzima u obzir učinak IKT usluga kojima se podupiru ključne ili važne funkcije, a koje pružaju treće strane pružatelji IKT usluga na financijski subjekt i svi rizici koje predstavljaju te IKT usluge kojima se podupiru ključne ili važne funkcije, a koje pružaju treće strane pružatelji IKT usluga, uključujući sljedeće:

(a) operativne rizike;

(b) pravne rizike;

(c) IKT rizike;

(d) reputacijske rizike;

(e) rizike povezane sa zaštitom povjerljivih ili osobnih podataka;

(f) rizike povezane s dostupnošću podataka;

(g) rizike povezane s lokacijom na kojoj se podaci obrađuju i pohranjuju;

(h) rizike povezani s lokacijom treće strane pružatelja IKT usluga;

(i) koncentracijske IKT rizike na razini subjekta.

Članak 6.

Dubinska analiza

1. Politikom se utvrđuje primjeren i razmjeran postupak za odabir i ocjenjivanje potencijalnih trećih strana pružatelja IKT usluga, uzimajući pritom u obzir je li treća strana pružatelj IKT usluga pružatelj IKT usluga unutar grupe, te se od financijskog subjekta zahtijeva da prije sklapanja ugovora ocijeni sljedeća obilježja treće strane pružatelja IKT usluga:

(a) ima li poslovni ugled, dostatne sposobnosti, stručno znanje i odgovarajuće financijske, ljudske i tehničke resurse, standarde informacijske sigurnosti, odgovarajuću organizacijsku strukturu, postupke upravljanje rizicima i unutarnje kontrole te, ako je primjenjivo, potrebna odobrenja ili registracije za pouzdano i profesionalno pružanje IKT usluga kojima se podupire ključna ili važna funkcija;

(b) može li pratiti relevantna tehnološka dostignuća i prepoznati vodeću praksu u području sigurnosti IKT-a te je provesti, ako je to potrebno, kako bi se uspostavio učinkovit i pouzdan okvir za digitalnu operativnu otpornost;

(c) angažira li ili namjerava angažirati podugovaratelje za pružanje IKT usluga kojima se podupiru ključne ili važne funkcije ili njihovi bitni dijelovi;

(d) nalazi li se ili obrađuje li ili pohranjuje podatke u trećoj zemlji i, ako je to slučaj, povećava li se tom praksom razina operativnih rizika, reputacijskih rizika ili rizika od utjecaja restriktivnih mjera, među ostalim od embarga i sankcija, koji mogu utjecati na sposobnost treće strane pružatelja IKT usluga da pruža IKT usluge ili financijskog subjekta da primi te IKT usluge;

(e) pristaje li na ugovorne aranžmane kojima se osigurava da sam financijski subjekt, imenovane treće strane i nadležna tijela mogu učinkovito provoditi revizije treće strane pružatelja IKT usluga, među ostalim na licu mjesta;

(f) djeluje li na etički i društveno odgovoran način, poštuje li ljudska prava i prava djece, uključujući zabranu dječjeg rada, poštuje li primjenjiva načela zaštite okoliša i osigurava li odgovarajuće radne uvjete.

2. Politikom se utvrđuje potrebna razina jamstva u pogledu djelotvornosti okvira za upravljanje rizicima trećih strana pružatelja IKT usluga za IKT usluge kojima se podupiru ključne ili važne funkcije koje pruža treća strana pružatelj IKT usluga. Politikom se zahtijeva da postupak dubinske analize uključuje ocjenu postojanja mjera za smanjenje rizika i mjera za kontinuitet poslovanja te načina na koji je njihova primjena osigurana u trećoj strani pružatelju IKT usluga.

3. Politikom se utvrđuje postupak dubinske analize za odabir i ocjenu potencijalnih trećih strana pružatelja IKT usluga te se navodi koje od sljedećih elemenata treba upotrebljavati za potrebnu razinu jamstva u pogledu rada treće strane pružatelja IKT usluga:

(a) revizije ili neovisne procjene koje provodi sam financijski subjekt ili se provode u njegovo ime;

(b) izvješća o neovisnoj reviziji koja na zahtjev podnosi treća strana pružatelj IKT usluga;

(c) revizorska izvješća koja izrađuje funkcija unutarnje revizije treće strane pružatelja IKT usluga;

(d) odgovarajući certifikati trećih strana;

(e) druge relevantne informacije dostupne financijskom subjektu ili druge informacije koje dostavlja treća strana pružatelj IKT usluga.

4. Financijski subjekti osiguravaju odgovarajuću razinu jamstva u pogledu rada treće strane pružatelja IKT usluga, uzimajući u obzir elemente iz stavka 3. točaka od (a) do (e). Prema potrebi, upotrebljava se više elemenata iz tih točaka.

Članak 7.

Sukobi interesa

1. U politici se utvrđuju odgovarajuće mjere za prepoznavanje, sprečavanje i upravljanje stvarnim ili mogućim sukobima interesa koji proizlaze iz angažiranja trećih strana pružatelja IKT usluga, koje treba poduzeti prije sklapanja relevantnih ugovornih aranžmana te se predviđa stalno praćenje tih sukoba interesa.

2. Ako IKT usluge kojima se podupiru ključne ili važne funkcije pružaju pružatelji IKT usluga unutar grupe, u politici se navodi da se odluke o uvjetima IKT usluga, uključujući financijske uvjete, donose objektivno.

Članak 8.

Ugovorne klauzule

1. U politici se utvrđuje da relevantni ugovorni aranžman mora biti u pisanom obliku i uključivati sve elemente iz članka 30. stavaka 2. i 3. Uredbe (EU) 2022/2554. Politika uključuje i elemente koji se odnose na zahtjeve iz članka 1. stavka 1. točke (a) Uredbe (EU) 2022/2554 te, prema potrebi, drugog relevantnog prava Unije i nacionalnog prava.

2. U politici se navodi da relevantni ugovorni aranžmani uključuju pravo financijskog subjekta na pristup informacijama, provođenje inspekcija i revizija te provođenje testiranja IKT-a. Ne dovodeći u pitanje konačnu odgovornost financijskog subjekta, u tu svrhu politikom se zahtijeva da financijski subjekt primjenjuje sljedeće metode:

(a) vlastite unutarnje revizije ili revizije koje provode imenovane treće strane;

(b) prema potrebi, skupne revizije i skupna testiranja IKT-a, uključujući penetracijsko testiranje vođeno prijetnjama, koje organizira zajedno s drugim financijskim subjektima ili društvima koji upotrebljavaju IKT usluge iste treće strane pružatelja IKT usluga i koje provode ti financijski subjekti ili društva naručitelji odnosno treća strana koju su oni imenovali;

(c) prema potrebi, certifikate koje izrađuju treće strane;

(d) prema potrebi, izvješća o unutarnjoj reviziji ili izvješća o reviziji treće strane koja izrađuju treće strane pružatelji IKT usluga.

3. Financijski subjekt s vremenom se ne oslanja isključivo na certifikate iz stavka 2. točke (c) ili izvješća o reviziji iz točke (d) tog stavka. Politikom se primjena metoda iz stavka 2. točaka (c) i (d) dopušta samo ako financijski subjekt:

(a) zadovoljan je planom revizije treće strane pružatelja IKT usluga o relevantnim ugovornim aranžmanima;

(b) osigurava da certifikati ili izvješća o reviziji obuhvaćaju sustave i ključne kontrole koje je utvrdio te usklađenost s relevantnim regulatornim zahtjevima;

(c) temeljito i kontinuirano ocjenjuje sadržaj certifikata ili izvješća o reviziji i provjerava jesu li izvješća ili certifikati zastarjeli;

(d) osigurava da su ključni sustavi i kontrole obuhvaćeni budućim verzijama certifikata ili izvješća o reviziji;

(e) zadovoljan je sposobnošću stranke koja izdaje certifikate ili provodi reviziju;

(f) zadovoljan je jer se certifikati izdaju i revizije provode u skladu s općepriznatim relevantnim profesionalnim standardima te uključuju ispitivanje operativne učinkovitosti uspostavljenih ključnih kontrola;

(g) ima ugovorno pravo zahtijevati, s učestalošću koja je razumna i opravdana sa stajališta upravljanja rizikom, da se certifikati ili izvješća o reviziji izmijene kako bi uključivali druge relevantne sustave i kontrole;

(h) ima ugovorno pravo po vlastitom nahođenju provoditi pojedinačne i skupne revizije ugovornih aranžmana i izvršavati to pravo s dogovorenom učestalošću.

4. Politikom se osigurava da se bitne promjene ugovornih aranžmana formaliziraju u pisanom dokumentu koji su datirale i potpisale sve stranke te se u njoj utvrđuje postupak obnove ugovornih aranžmana.

Članak 9.

Praćenje ugovornih aranžmana

1. Politikom se zahtijeva da se u ugovornim aranžmanima utvrde mjere i ključni pokazatelji za kontinuirano praćenje rada trećih strana pružatelja IKT usluga, uključujući mjere za praćenje usklađenosti sa zahtjevima u pogledu povjerljivosti, dostupnosti, cjelovitosti i vjerodostojnosti podataka i informacija te usklađenosti trećih strana pružatelja IKT usluga s relevantnim politikama i postupcima financijskog subjekta. U politici se utvrđuju i mjere koje se primjenjuju kad sporazumi o razini usluga nisu ispoštovani, uključujući prema potrebi ugovorne kazne.

2. U politici se utvrđuje kako financijski subjekt ocjenjuje ispunjavaju li treće strane pružatelji IKT usluga angažirane za pružanje IKT usluga kojima se podupiru ključne ili važne funkcije odgovarajuće standarde rada i kvalitete u skladu s ugovornim aranžmanom i politikama financijskog subjekta. Politikom se posebno osigurava sljedeće:

(a) da treće strane pružatelji IKT usluga financijskom subjektu dostavljaju odgovarajuća izvješća o svojim aktivnostima i uslugama, uključujući periodična izvješća, izvješća o incidentima, izvješća o pružanju usluga, izvješća o sigurnosti IKT-a te izvješća o mjerama kontinuiteta poslovanja i provedenim testovima;

(b) da se rad trećih strana pružatelja IKT usluga ocjenjuje ključnim pokazateljima uspješnosti, ključnim pokazateljima kontrole, revizijama, samocertificiranjem i neovisnim preispitivanjima u skladu s okvirom financijskog subjekta za upravljanje IKT rizicima;

(c) da financijski subjekt prima druge relevantne informacije od treće strane pružatelja IKT usluga;

(d) da financijski subjekt bude obaviješten, prema potrebi, o IKT incidentima i operativnim ili sigurnosnim incidentima povezanima s plaćanjem;

(e) da se provode neovisna preispitivanja i revizije kojima se provjerava usklađenost s pravnim i regulatornim zahtjevima i politikama.

3. U politici se utvrđuje da procjenu iz stavka 2. treba dokumentirati, a njezine rezultate upotrebljavati za ažuriranje procjene rizika financijskog subjekta iz članka 6.

4. Politikom se utvrđuju odgovarajuće mjere koje financijski subjekt treba poduzeti ako utvrdi propuste treće strane pružatelja IKT usluga, uključujući IKT incidente i operativne ili sigurnosne incidente povezane s plaćanjem, u pružanju IKT usluga kojima se podupiru ključne ili važne funkcije ili u usklađenosti s ugovornim aranžmanima ili pravnim zahtjevima. U politici se utvrđuje i način na koji se prati provedba tih mjera kako bi se osiguralo da ih se zaista poštuje, uzimajući u obzir značajnost propusta.

Članak 10.

Povlačenje iz ugovornih aranžmana i njihov raskid

Politika sadržava zahtjeve za dokumentirani izlazni plan za svaki ugovorni aranžman te za periodično preispitivanje i testiranje tog plana. Pri utvrđivanju izlaznog plana u obzir se uzima sljedeće:

(a) nepredviđeni i trajni prekidi u pružanju usluga;

(b) neodgovarajuće ili neuspješno pružanje usluga;

(c) neočekivani raskid ugovornog aranžmana.

Izlazni plan treba biti realističan, izvediv, utemeljen na uvjerljivim scenarijima i razumnim pretpostavkama te imati planirani raspored provedbe usklađen s uvjetima izlaska i raskida utvrđenima u ugovornim aranžmanima.

Članak 11.

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 13. ožujka 2024.

Za Komisiju
Predsjednica
Ursula VON DER LEYEN