Uradni list
Evropske unije

SL
Serija L

2024/1773

25.6.2024

DELEGIRANA UREDBA KOMISIJE (EU) 2024/1773

z dne 13. marca 2024

o dopolnitvi Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta v zvezi z regulativnimi tehničnimi standardi za nadaljnjo opredelitev podrobne vsebine politike v zvezi s pogodbenimi dogovori o uporabi storitev IKT, ki podpirajo kritične ali pomembne funkcije in ki jih opravljajo tretji ponudniki storitev IKT

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 ([1]) ter zlasti člena 28(10), tretji pododstavek, Uredbe,

ob upoštevanju naslednjega:

(1) Okvir za digitalno operativno odpornost za finančni sektor, vzpostavljen z Uredbo (EU) 2022/2554, zahteva, da finančni subjekti določijo nekatera ključna načela za obvladovanje tveganja tretjih oseb na področju IKT, ki so zlasti pomembna, kadar finančni subjekti za podporo pri svojih kritičnih ali pomembnih funkcijah sodelujejo s tretjimi ponudniki storitev IKT.

(2) Finančni subjekti morajo kot del svojega okvira za obvladovanje tveganj na področju IKT sprejeti in redno pregledovati strategijo o tveganjih tretjih oseb na področju IKT. V skladu s členom 28(2) Uredbe (EU) 2022/2554 navedena strategija vključuje politiko o uporabi storitev IKT, ki podpirajo kritične ali pomembne funkcije in ki jih zagotavljajo tretji ponudniki storitev IKT. Uporablja se na posamični ter, kadar je ustrezno, na subkonsolidirani in konsolidirani podlagi.

(3) Finančni subjekti se zelo razlikujejo po velikosti, strukturi in notranji organizaciji ter po naravi in kompleksnosti svojih dejavnosti in poslovanja. Pri oblikovanju politike v zvezi s pogodbenimi dogovori o uporabi storitev IKT, ki podpirajo kritične ali pomembne funkcije, s strani tretjih ponudnikov IKT (v nadaljnjem besedilu: politika), je treba upoštevati to raznolikost, hkrati pa uvesti nekatere temeljne regulativne zahteve, ki so primerne za vse finančne subjekte, in zagotoviti, da se te zahteve uporabljajo sorazmerno.

(4) Kadar finančni subjekti pripadajo skupini, bi moralo obvladujoče podjetje, ki je odgovorno za zagotavljanje konsolidiranih ali subkonsolidiranih računovodskih izkazov za skupino, zagotoviti, da se politika v skupini uporablja dosledno in skladno.

(5) Pri uporabi politike bi bilo treba ponudnike storitev IKT znotraj skupine, vključno s tistimi, ki so v celoti ali skupno v lasti finančnih subjektov v okviru iste institucionalne sheme za zaščito vlog, šteti za tretje ponudnike storitev IKT. Tveganja, ki jih predstavljajo ponudniki storitev IKT znotraj skupine, so lahko različna, vendar so zahteve, ki se zanje uporabljajo, v skladu z Uredbo (EU) 2022/2554 enake. Podobno bi se morala politika uporabljati tudi za podizvajalce, ki opravljajo storitve IKT, ki podpirajo kritične ali pomembne funkcije ali njihove bistvene dele, za tretje ponudnike storitev IKT, kadar obstaja veriga tretjih ponudnikov storitev IKT.

(6) Končna odgovornost upravljalnega organa pri obvladovanju tveganja finančnega subjekta na področju IKT je splošno načelo, ki se uporablja tudi v zvezi z uporabo tretjih ponudnikov storitev IKT. To odgovornost bi bilo treba nadalje prenesti v stalno sodelovanje upravljalnega organa pri nadzoru in spremljanju obvladovanja tveganj na področju IKT, vključno s sprejetjem in pregledom politike vsaj enkrat letno.

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

(7) Za zagotovitev ustreznega poročanja upravljalnemu organu bi bilo treba v politiki jasno določiti in opredeliti notranje odgovornosti za odobritev, upravljanje, nadzor in dokumentiranje pogodbenih dogovorov o uporabi storitev IKT, ki podpirajo kritične ali pomembne funkcije in ki jih zagotavljajo tretji ponudniki storitev IKT (v nadaljnjem besedilu: pogodbeni dogovori), vključno s storitvami IKT, ki se zagotavljajo na podlagi pogodbenih dogovorov iz člena 28(1), točka (a), Uredbe (EU) 2022/2554.

(8) Da bi se upoštevala vsa možna tveganja, ki se lahko pojavijo pri sklepanju pogodb za storitve IKT, ki podpirajo kritično ali pomembno funkcijo, bi morala struktura politike za pogodbene dogovore s tretjimi ponudniki slediti vsem korakom vsake glavne faze življenjskega cikla.

(9) Za zmanjšanje identificiranih tveganj bi bilo treba v politiki določiti načrtovanje pogodbenih dogovorov, vključno z oceno tveganja, skrbnim pregledom in postopkom odobritve za nove ali pomembne spremembe teh pogodbenih dogovorov. Za obvladovanje tveganj, ki se lahko pojavijo pred sklenitvijo pogodbenega dogovora s tretjim ponudnikom storitev IKT, bi bilo treba v politiki določiti ustrezen in sorazmeren postopek za izbor in oceno primernosti potencialnih tretjih ponudnikov storitev IKT ter zahtevati, da finančni subjekt upošteva neizčrpen seznam elementov, ki bi jih morali imeti vzpostavljene tretji ponudniki storitev IKT. Seznam bi moral vključevati elemente, povezane s poslovnim ugledom ponudnikov storitev, njihovimi finančnimi, človeškimi in tehničnimi viri, informacijsko varnostjo, organizacijsko strukturo, vključno z obvladovanjem tveganj, in notranjimi kontrolami.

(10) Za zagotovitev zanesljivega obvladovanja tveganja pri opravljanju storitev IKT, ki podpirajo kritične ali pomembne funkcije, s strani tretjih ponudnikov storitev IKT, bi morala politika vsebovati informacije o izvajanju, spremljanju in upravljanju pogodbenih dogovorov, tudi na konsolidirani in subkonsolidirani ravni, kadar je ustrezno. To vključuje zahteve za pogodbene klavzule o vzajemnih obveznostih finančnih subjektov in tretjih ponudnikov storitev IKT, ki bi morale biti pisno določene. Da bi zagotovili učinkovit nadzor in spodbudili odpornost v primeru sprememb poslovnega modela ali poslovnega okolja, bi morala politika finančnim subjektom ali imenovanim tretjim osebam in pristojnim organom zagotoviti pravice do inšpekcijskih pregledov in dostopa do informacij ter dodatno opredeliti izhodne strategije in postopke odpovedi.

(11) Če osebne podatke obdelujejo tretji ponudniki storitev IKT, ta politika in pogodbeni dogovori ne posegajo v obveznosti iz Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta ([2]) in bi jih morali dopolnjevati, kot so sklenitev pisne pogodbe, ki opisuje obdelavo osebnih podatkov, zahteva po zagotavljanju varnosti obdelave osebnih podatkov in določitev vseh drugih elementov, ki se zahtevajo v skladu z navedeno uredbo.

([2]) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) Skupni odbor evropskih nadzornih organov iz člena 54 Uredbe (EU) št. 1093/2010 Evropskega parlamenta in Sveta ([3]), člena 54 Uredbe (EU) št. 1094/2010 Evropskega parlamenta in Sveta ([4]) ter člena 54 Uredbe (EU) št. 1095/2010 Evropskega parlamenta in Sveta ([5]) je organiziral odprta javna posvetovanja o osnutku regulativnih tehničnih standardov, na katerem temelji ta uredba, analiziral morebitne stroške in koristi predlaganih standardov ter zaprosil za nasvet interesno skupino za bančništvo, ustanovljeno v skladu s členom 37 Uredbe (EU) št. 1093/2010, interesno skupino za zavarovanja in pozavarovanja ter interesno skupino za poklicne pokojninske sklade, ustanovljeni v skladu s členom 37 Uredbe (EU) št. 1094/2010, ter interesno skupino za vrednostne papirje in trge, ustanovljeno v skladu s členom 37 Uredbe (EU) št. 1095/2010.

(13) V skladu s členom 42(1) Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta ([6]) je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je mnenje podal 24. januarja 2024 –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Splošni profil tveganja in kompleksnost

Politika o uporabi storitev IKT, ki podpirajo kritične ali pomembne funkcije in ki jih opravljajo tretji ponudniki storitev IKT (v nadaljnjem besedilu: politika), upošteva velikost in splošni profil tveganja finančnega subjekta ter naravo, obseg in elemente povečane ali zmanjšane kompleksnosti njegovih storitev, dejavnosti in poslovanja, vključno z elementi, ki se nanašajo na:

(a) vrsto storitev IKT, vključenih v pogodbeni dogovor o uporabi storitev IKT, ki podpirajo kritične ali pomembne funkcije in ki jih opravljajo tretji ponudniki storitev IKT (v nadaljnjem besedilu: pogodbeni dogovor), med finančnim subjektom in tretjim ponudnikom storitev IKT;

(b) lokacijo tretjega ponudnika storitev IKT ali lokacijo njegovega obvladujočega podjetja;

(c) to, ali storitve IKT, ki podpirajo kritične ali pomembne funkcije, opravlja tretji ponudnik storitev IKT, ki se nahaja v državi članici ali tretji državi, tudi ob upoštevanju lokacije, s katere se opravljajo storitve IKT, ter lokacije, kjer se obdelujejo in shranjujejo podatki;

(d) naravo podatkov, ki se izmenjujejo s tretjim ponudnikom storitev IKT;

(e) to, ali je tretji ponudnik storitev IKT del iste skupine kot finančni subjekt, za katerega se opravljajo storitve;

([3]) Uredba (EU) št. 1093/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski bančni organ) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/78/ES (UL L 331, 15.12.2010, str. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Uredba (EU) št. 1094/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski organ za zavarovanja in poklicne pokojnine) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/79/ES (UL L 331, 15.12.2010, str. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Uredba (EU) št. 1095/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski organ za vrednostne papirje in trge) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/77/ES (UL L 331, 15.12.2010, str. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(f) uporabo tretjih ponudnikov storitev IKT, ki so pooblaščeni, registrirani ali so pod nadzorom ali pregledom pristojnega organa v državi članici ali za katere velja okvir nadzora v skladu s poglavjem V, oddelek II, Uredbe (EU) 2022/2554, in uporabo tretjih ponudnikov storitev IKT, ki to niso;

(g) uporabo tretjih ponudnikov storitev IKT, ki so pooblaščeni, registrirani ali so pod nadzorom ali pregledom nadzornega organa v tretji državi, in uporabo tretjih ponudnikov storitev IKT, ki to niso;

(h) to, ali je opravljanje storitev IKT, ki podpirajo kritične ali pomembne funkcije, koncentrirano pri enem tretjem ponudniku storitev IKT ali majhnem številu takih ponudnikov storitev;

(i) prenosljivost storitev IKT, ki podpirajo kritične ali pomembne funkcije, na drugega tretjega ponudnika storitev IKT, tudi zaradi tehnoloških posebnosti;

(j) morebitni vpliv motenj pri opravljanju storitev IKT, ki podpirajo kritične ali pomembne funkcije, na neprekinjenost dejavnosti finančnega subjekta in razpoložljivost njegovih storitev.

Člen 2

Uporaba v skupini

Kadar se ta uredba uporablja na subkonsolidirani ali konsolidirani podlagi, obvladujoče podjetje, ki je odgovorno za zagotavljanje konsolidiranih ali subkonsolidiranih računovodskih izkazov za skupino, zagotovi, da se politika dosledno izvaja v vseh finančnih subjektih, ki so del skupine, in da je ustrezna za učinkovito uporabo te uredbe na vseh ustreznih ravneh skupine.

Člen 3

Ureditve upravljanja

1. Upravljalni organ politiko pregleda vsaj enkrat letno in jo po potrebi posodobi. Spremembe politike se izvedejo pravočasno in takoj, ko je to mogoče v okviru ustreznih pogodbenih dogovorov. Finančni subjekt dokumentira načrtovani časovni okvir za izvedbo.

2. V politiki se določi ali se sklicuje na metodologijo za določanje, katere storitve IKT podpirajo kritične ali pomembne funkcije. V politiki je določeno tudi, kdaj je treba to oceno izvesti in pregledati.

3. Politika jasno določi notranje odgovornosti za odobritev, upravljanje, nadzor in dokumentiranje ustreznih pogodbenih dogovorov ter zagotavlja, da se v finančnem subjektu ohranijo ustrezne spretnosti, izkušnje in znanje za učinkovit nadzor ustreznih pogodbenih dogovorov, vključno s storitvami IKT, ki se opravljajo v skladu s temi dogovori.

4. Brez poseganja v končno odgovornost finančnega subjekta za učinkovit nadzor nad ustreznimi pogodbenimi dogovori se v skladu s politiko zahteva, da se ocenjuje, ali ima tretji ponudnik storitev IKT dovolj virov za zagotovitev, da finančni subjekt izpolnjuje vse svoje pravne in regulativne zahteve v zvezi s storitvami IKT, ki se opravljajo in podpirajo kritične ali pomembne funkcije.

5. V politiki se jasno opredeli funkcija ali član višjega vodstva, odgovoren za spremljanje ustreznih pogodbenih dogovorov. Politika določa, kako naj ta funkcija ali član višjega vodstva sodeluje z nadzornimi funkcijami, razen če je njihov del, ter določa linije poročanja upravljalnemu organu, vključno z naravo informacij, ki jih je treba poročati, in dokumenti, ki jih je treba predložiti. Z njo se določi tudi pogostost takega poročanja.

6. Politika zagotavlja, da so pogodbeni dogovori skladni z naslednjim:

(a) okvirom za obvladovanje tveganj na področju IKT iz člena 6 Uredbe (EU) 2022/2554;

(b) politiko informacijske varnosti iz člena 9(4) Uredbe (EU) 2022/2554;

(c) politiko neprekinjenega poslovanja na področju IKT iz člena 11 Uredbe (EU) 2022/2554;

(d) zahtevami v zvezi s poročanjem o incidentih iz člena 19 Uredbe (EU) 2022/2554.

7. Politika zahteva, da se storitve IKT, ki podpirajo kritične ali pomembne funkcije in ki jih opravljajo tretji ponudniki storitev IKT, neodvisno pregledajo in vključijo v revizijski načrt.

8. V politiki je izrecno navedeno, da pogodbeni dogovori:

(a) finančnega subjekta in njegovega upravljalnega organa ne razrešujejo njegovih regulativnih obveznosti in odgovornosti do njegovih strank;

(b) ne preprečujejo učinkovitega nadzora nad finančnim subjektom in niso v nasprotju z nadzornimi omejitvami glede storitev in dejavnosti;

(c) zahtevajo, da tretji ponudniki storitev IKT sodelujejo s pristojnimi organi;

(d) zahtevajo, da imajo finančni subjekt, njegovi revizorji in pristojni organi učinkovit dostop do podatkov in prostorov v zvezi z uporabo storitev IKT, ki podpirajo kritične ali pomembne funkcije.

Člen 4

Glavne faze življenjskega cikla za sprejetje in uporabo pogodbenih dogovorov

Politika določa zahteve, vključno s pravili, odgovornostmi in postopki, za vsako glavno fazo življenjskega cikla pogodbenega dogovora, ki zajemajo vsaj naslednje:

(a) odgovornosti upravljalnega organa, vključno z njegovo vključenostjo, kot je primerno, v postopek odločanja o uporabi storitev IKT, ki podpirajo kritične ali pomembne funkcije in ki jih zagotavljajo tretji ponudniki storitev IKT;

(b) načrtovanje pogodbenih dogovorov, vključno z oceno tveganja, skrbnim pregledom iz členov 5 in 6 ter postopkom odobritve v zvezi z novimi ali pomembnimi spremembami pogodbenih dogovorov iz člena 8(4);

(c) sodelovanje poslovnih enot, notranjih kontrol in drugih ustreznih enot v zvezi s pogodbenimi dogovori;

(d) izvajanje, spremljanje in upravljanje pogodbenih dogovorov iz členov 7, 8 in 9, tudi na konsolidirani in subkonsolidirani ravni, kadar je ustrezno;

(e) dokumentacijo in vodenje evidenc ob upoštevanju zahtev v zvezi z registrom informacij iz člena 28(3) Uredbe (EU) 2022/2554;

(f) izhodne strategije in postopke odpovedi iz člena 10.

Člen 5

Predhodna ocena tveganja

1. Politika zahteva, da se poslovne potrebe finančnega subjekta opredelijo pred sklenitvijo pogodbenega dogovora.

2. Politika zahteva, da se ocena tveganja izvede na ravni finančnega subjekta ter, kadar je ustrezno, na konsolidirani in subkonsolidirani ravni pred sklenitvijo pogodbenega dogovora.

Pri oceni tveganja se upoštevajo vse ustrezne zahteve iz Uredbe (EU) 2022/2554 in veljavne sektorske zakonodaje Unije. Zlasti se upošteva učinek opravljanja storitev IKT, ki podpirajo kritične ali pomembne funkcije, s strani tretjih ponudnikov storitev IKT na finančni subjekt in vsa tveganja, ki jih predstavlja opravljanje teh storitev IKT, ki podpirajo kritične ali pomembne funkcije, s strani tretjih ponudnikov storitev IKT, vključno z naslednjim:

(a) operativna tveganja;

(b) pravna tveganja;

(c) tveganja na področju IKT;

(d) tveganje izgube ugleda;

(e) tveganja, povezana z varstvom zaupnih ali osebnih podatkov;

(f) tveganja, povezana razpoložljivostjo podatkov;

(g) tveganja, povezana z lokacijo, kjer se podatki obdelujejo in shranjujejo;

(h) tveganja, povezana z lokacijo tretjega ponudnika storitev IKT;

(i) tveganja koncentracije na področju IKT na ravni subjekta.

Člen 6

Skrbni pregled

1. Politika določi ustrezen in sorazmeren postopek za izbiro in ocenjevanje potencialnih tretjih ponudnikov storitev IKT ob upoštevanju, ali je tretji ponudnik storitev IKT ponudnik storitev IKT znotraj skupine ali ne, ter zahteva, da finančni subjekt pred sklenitvijo pogodbenega dogovora oceni, ali tretji ponudnik storitev IKT:

(a) ima poslovni ugled, zadostne sposobnosti, strokovno znanje ter ustrezne finančne, človeške in tehnične vire, standarde informacijske varnosti, ustrezno organizacijsko strukturo, obvladovanje tveganj in notranje kontrole ter, kadar je ustrezno, potrebna dovoljenja ali registracije za zanesljivo in strokovno opravljanje storitev IKT, ki podpirajo kritično ali pomembno funkcijo;

(b) je sposoben spremljati zadevni tehnološki razvoj in opredeliti vodilne prakse na področju varnosti IKT ter jih izvajati, kadar je primerno, da ima učinkovit in trden okvir za digitalno operativno odpornost;

(c) za opravljanje storitev IKT, ki podpirajo kritične ali pomembne funkcije, ali njihove bistvene dele, uporablja ali namerava uporabljati podizvajalce IKT;

(d) se nahaja ali obdeluje ali shranjuje podatke v tretji državi in, če je tako, ali ta praksa vpliva na raven operativnega tveganja ali tveganja izgube ugleda ali na tveganje, da bi nanj vplivali omejevalni ukrepi, vključno z embargom in sankcijami, ki lahko vplivajo na zmožnost tretjega ponudnika storitev IKT, da opravlja storitve IKT, ali finančnega subjekta, da prejme te storitve IKT;

(e) soglaša s pogodbenimi dogovori, ki zagotavljajo, da lahko finančni subjekt sam, imenovane tretje osebe in pristojni organi dejansko opravijo revizije pri tretjem ponudniku storitev IKT, tudi na kraju samem;

(f) deluje etično in družbeno odgovorno, spoštuje človekove pravice in pravice otrok, vključno s prepovedjo dela otrok, spoštuje veljavna načela varstva okolja in zagotavlja ustrezne delovne pogoje.

2. V politiki se določi zahtevana raven zanesljivosti v zvezi z učinkovitostjo okvira tretjih ponudnikov storitev IKT za obvladovanje tveganj za storitve IKT, ki podpirajo kritične ali pomembne funkcije in ki jih bo opravljal tretji ponudnik storitev IKT. Politika zahteva, da postopek skrbnega pregleda vključuje oceno obstoja ukrepov za zmanjšanje tveganja in neprekinjeno poslovanje ter kako je zagotovljeno njihovo delovanje v okviru tretjega ponudnika storitev IKT.

3. V politiki se določi postopek skrbnega pregleda za izbiro in ocenjevanje potencialnih tretjih ponudnikov storitev IKT ter navede, katerega od naslednjih elementov je treba uporabiti za zahtevano raven zanesljivosti glede uspešnosti tretjega ponudnika storitev IKT:

(a) revizije ali neodvisne ocene, ki jih izvede finančni subjekt sam ali se opravijo v njegovem imenu;

(b) neodvisna revizijska poročila, ki jih na zahtevo predloži tretji ponudnik storitev IKT;

(c) revizijska poročila, ki jih pripravi funkcija notranje revizije tretjega ponudnika storitev IKT;

(d) ustrezna potrdila tretjih oseb;

(e) druge ustrezne informacij, ki so na voljo finančnemu subjektu, ali druge informacije, ki jih zagotovi tretji ponudnik storitev IKT.

4. Finančni subjekti zagotovijo ustrezno raven zanesljivosti glede uspešnosti tretjega ponudnika storitev IKT ob upoštevanju elementov iz odstavka 3, točke (a) do (e). Kadar je primerno, se uporabi več kot en element iz navedenih točk.

Člen 7

Nasprotja interesov

1. V politiki se določi ustrezne ukrepe za identifikacijo, preprečevanje in obvladovanje dejanskih ali morebitnih nasprotij interesov, ki izhajajo iz uporabe tretjih ponudnikov storitev IKT, ki jih je treba sprejeti pred sklenitvijo ustreznih pogodbenih dogovorov, in zagotovi stalno spremljanje takih nasprotij interesov.

2. Kadar storitve IKT, ki podpirajo kritične ali pomembne funkcije, opravljajo ponudniki storitev IKT znotraj skupine, se v politiki določi, da se odločitve o pogojih, vključno s finančnimi pogoji, za storitve IKT sprejemajo objektivno.

Člen 8

Pogodbene klavzule

1. V politiki se določi, da mora biti zadevni pogodbeni dogovor v pisni obliki in mora vključevati vse elemente iz člena 30(2) in (3) Uredbe (EU) 2022/2554. Politika vključuje tudi elemente v zvezi z zahtevami iz člena 1(1), točka (a), Uredbe (EU) 2022/2554 ter, kot je ustrezno, drugega ustreznega prava Unije in nacionalnega prava.

2. Politika določa, da morajo ustrezni pogodbeni dogovori vključevati pravico finančnega subjekta do dostopa do informacij, izvajanja inšpekcijskih pregledov in revizij ter izvajanja testiranja IKT. V ta namen politika zahteva, da finančni subjekt uporablja naslednje metode, brez poseganja v končno odgovornost finančnega subjekta:

(a) svojo notranjo revizijo ali revizijo, ki jo opravi imenovana tretja oseba;

(b) kadar je primerno, skupne revizije in skupno testiranje IKT, vključno s penetracijskim testiranjem na podlagi groženj, ki se organizirajo skupaj z drugimi finančnimi subjekti ali podjetji naročniki, ki uporabljajo storitve IKT istega tretjega ponudnika storitev IKT, in ki jih izvedejo navedeni finančni subjekti ali podjetja naročniki ali tretja oseba, ki jo ti imenujejo;

(c) kadar je primerno, potrdila tretjih oseb;

(d) kadar je primerno, notranja revizijska poročila ali revizijska poročila tretje osebe, ki jih da na voljo tretji ponudnik storitev IKT.

3. Finančni subjekt se po določenem času ne zanaša zgolj na potrdila iz odstavka 2, točka (c), ali revizijska poročila iz točke (d) navedenega odstavka. Politika dovoljuje uporabo metod iz odstavka 2, točki (c) in (d), samo kadar finančni subjekt:

(a) meni, da je revizijski načrt tretjega ponudnika storitev IKT za ustrezne pogodbene dogovore zadovoljiv;

(b) zagotavlja, da obseg potrdil ali revizijskih poročil zajema sisteme in ključne kontrole, ki jih opredeljuje, ter zagotavlja skladnost z ustreznimi regulativnimi zahtevami;

(c) redno temeljito ocenjuje vsebino potrdil ali revizijskih poročil in preveri, da poročila ali potrdila niso zastarela;

(d) zagotavlja, da so ključni sistemi in kontrole zajeti v prihodnjih različicah potrdila ali revizijskega poročila;

(e) meni, da je certifikacijski ali revizijski organ dovolj usposobljen;

(f) meni, da se potrdila izdajajo in da se revizije izvajajo v skladu s splošno priznanimi ustreznimi strokovnimi standardi ter vključujejo test operativne učinkovitosti vzpostavljenih ključnih kontrol;

(g) ima pogodbeno pravico, da tako pogosto, kot je razumno in zakonito z vidika obvladovanja tveganja, zahteva spremembe obsega potrdil ali revizijskih poročil, tako da so zajeti drugi ustrezni sistemi in kontrole;

(h) ima pogodbeno pravico do izvajanja posameznih in skupnih revizij po lastni presoji v zvezi s pogodbenimi dogovori in do izvajanja teh pravic v skladu z dogovorjeno pogostostjo.

4. Politika zagotavlja, da se pomembne spremembe pogodbenega dogovora formalizirajo v pisnem dokumentu, ki je datiran in ga podpišejo vse stranke, ter določa postopek podaljšanja pogodbenih dogovorov.

Člen 9

Spremljanje pogodbenih dogovorov

1. Politika zahteva, da se v pogodbenih dogovorih določijo ukrepi in ključni kazalniki za stalno spremljanje uspešnosti tretjih ponudnikov storitev IKT, vključno z ukrepi za spremljanje skladnosti z zahtevami glede zaupnosti, razpoložljivosti, celovitosti in avtentičnosti podatkov in informacij ter skladnosti tretjih ponudnikov storitev IKT z ustreznimi politikami in postopki finančnega subjekta. V politiki se določijo tudi ukrepi, ki se uporabljajo, kadar sporazumi o ravni storitev niso izpolnjeni, vključno s pogodbenimi kaznimi, kadar je to primerno.

2. Politika določa, kako mora finančni subjekt oceniti, ali tretji ponudniki storitev IKT, ki se uporabljajo za storitve IKT, ki podpirajo kritične ali pomembne funkcije, izpolnjujejo ustrezne standarde uspešnosti in kakovosti v skladu s pogodbenim dogovorom in lastnimi politikami finančnega subjekta. Politika zlasti zagotovi naslednje:

(a) da tretji ponudniki storitev IKT finančnemu subjektu predložijo ustrezna poročila o svojih dejavnostih in storitvah, vključno z rednimi poročili, poročili o incidentih, poročili o izvajanju storitev, poročili o varnosti IKT ter poročili o ukrepih za neprekinjeno poslovanje in testiranju neprekinjenega poslovanja;

(b) da se uspešnost tretjih ponudnikov storitev IKT ocenjuje s ključnimi kazalniki uspešnosti, ključnimi kontrolnimi kazalniki, revizijami, samopotrjevanjem in neodvisnimi pregledi v skladu z okvirom finančnega subjekta za obvladovanje tveganj na področju IKT;

(c) da finančni subjekt od tretjih ponudnikov storitev IKT prejme druge ustrezne informacije;

(d) da je finančni subjekt, kadar je primerno, obveščen o incidentih, povezanih z IKT, in operativnih ali varnostnih incidentih, povezanih s plačili;

(e) da se izvedejo neodvisni pregled in revizije, s katerimi se preverja skladnost s pravnimi in regulativnimi zahtevami in politikami.

3. Politika določa, da je treba oceno iz odstavka 2 dokumentirati, njeni rezultati pa se uporabijo za posodobitev ocene tveganja finančnega subjekta iz člena 6.

4. Politika določa ustrezne ukrepe, ki jih mora finančni subjekt sprejeti, če ugotovi pomanjkljivosti tretjih ponudnikov storitev IKT, vključno z incidenti, povezanimi z IKT, in operativnimi ali varnostnimi incidenti, povezanimi s plačili, pri opravljanju storitev IKT, ki podpirajo kritične ali pomembne funkcije, ali v skladu s pogodbenimi dogovori ali pravnimi zahtevami. Določa tudi, kako je treba spremljati izvajanje takih ukrepov, da se zagotovi njihovo učinkovito izpolnjevanje v določenem časovnem okviru, pri čemer se upošteva pomembnost pomanjkljivosti.

Člen 10

Prekinitev in odpoved pogodbenih dogovorov

Politika vsebuje zahteve za dokumentiran izhodni načrt za vsak pogodbeni dogovor ter za redni pregled in testiranje dokumentiranega izhodnega načrta. Pri določitvi izhodnega načrta je treba upoštevati:

(a) nepredvidene in vztrajne prekinitve storitev;

(b) neustrezno ali neuspešno zagotavljanje storitev;

(c) nepričakovano odpoved pogodbenega dogovora.

Izhodni načrt je realističen, izvedljiv, temelji na verjetnih scenarijih in razumnih predpostavkah ter ima načrtovan časovni razpored izvajanja, ki je združljiv s pogoji prekinitve in odpovedi, določenimi v pogodbenih dogovorih.

Člen 11

Začetek veljavnosti

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 13. marca 2024

Za Komisijo
predsednica
Ursula VON DER LEYEN