Evropski parlament
2019-2024

Dokument zasedanja

A9-0341/2021

7.12.2021

***I
POROČILO

o predlogu uredbe Evropskega parlamenta in Sveta o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014 in (EU) št. 909/2014
(COM(2020)0595 – C9-0304/2020 – 2020/0266(COD))

Odbor za ekonomske in monetarne zadeve

Poročevalec: Billy Kelleher

Oznake postopkov

*	Postopek posvetovanja
***	Postopek odobritve
***I	Redni zakonodajni postopek (prva obravnava)
***II	Redni zakonodajni postopek (druga obravnava)
***III	Redni zakonodajni postopek (tretja obravnava)

(Vrsta postopka je odvisna od pravne podlage, ki je predlagana v osnutku akta.)

Predlogi sprememb k osnutku akta

Spremembe, ki jih predlaga Parlament, v dveh stolpcih

Izbrisano besedilo je označeno s ***krepkim poševnim tiskom*** v levem stolpcu, zamenjano besedilo s ***krepkim poševnim tiskom*** v obeh stolpcih, novo besedilo pa s ***krepkim poševnim tiskom*** v desnem stolpcu.

Prva in druga vrstica glave vsakega predloga spremembe navajata zadevni del besedila v obravnavanem osnutku akta. Če predlog spremembe zadeva obstoječi akt, ki se ga želi spremeniti z osnutkom akta, glava poleg tega vsebuje še tretjo in četrto vrstico, ki navajata obstoječi akt oziroma zadevno določbo tega akta.

Spremembe, ki jih predlaga Parlament, v obliki konsolidiranega besedila

Novo besedilo je označeno s ***krepkim poševnim tiskom***. Izbrisano besedilo je označeno s simbolom ▌ ali prečrtano. Zamenjano besedilo je izbrisano ali prečrtano, besedilo, ki ga nadomešča, pa je označeno s ***krepkim poševnim tiskom***.
Izjema so spremembe izključno tehnične narave, ki so jih vnesle službe z namenom priprave končnega besedila in niso označene.

VSEBINA

Stran

OSNUTEK ZAKONODAJNE RESOLUCIJE EVROPSKEGA PARLAMENTA 5

OSNUTEK ZAKONODAJNE RESOLUCIJE EVROPSKEGA PARLAMENTA

o predlogu uredbe Evropskega parlamenta in Sveta o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014 in (EU) št. 909/2014
(COM(2020)0595 – C9-0304/2020 – 2020/0266(COD))

(Redni zakonodajni postopek: prva obravnava)

Evropski parlament,

– ob upoštevanju predloga Komisije Evropskemu parlamentu in Svetu (COM(2020)0595),

– ob upoštevanju člena 294(2) in člena 114 Pogodbe o delovanju Evropske unije, na podlagi katerih je Komisija podala predlog Parlamentu (C9-0304/2020),

– ob upoštevanju člena 294(3) Pogodbe o delovanju Evropske unije,

– ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora z dne 24. februarja 2021[1],

– ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora z dne ... [2],

– ob upoštevanju mnenja Evropske centralne banke z dne ... [3],

– ob upoštevanju člena 59 Poslovnika,

– ob upoštevanju poročila Odbora za ekonomske in monetarne zadeve (A9-0341/2021),

1. sprejme stališče v prvi obravnavi, kakor je določeno v nadaljevanju;

2. poziva Komisijo, naj mu zadevo ponovno predloži, če svoj predlog nadomesti, ga bistveno spremeni ali ga namerava bistveno spremeniti;

3. naroči svojemu predsedniku, naj stališče Parlamenta posreduje Svetu in Komisiji ter nacionalnim parlamentom.

[1] UL C 155, 30.4.2021, str. 38.
[2] UL C ... / Še ni objavljeno v Uradnem listu.
[3] UL C ... / Še ni objavljeno v Uradnem listu.

Predlog spremembe 1

PREDLOGI SPREMEMB EVROPSKEGA PARLAMENTA*

k predlogu Komisije

2020/0266(COD)

Predlog

UREDBE EVROPSKEGA PARLAMENTA IN SVETA

o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014 in (EU) št. 909/2014

(Besedilo velja za EGP)

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 114 Pogodbe,

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Evropske centralne banke,[4]

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora,[5]

v skladu z rednim zakonodajnim postopkom,

ob upoštevanju naslednjega:

(1) V digitalni dobi informacijska in komunikacijska tehnologija (IKT) podpira zapletene sisteme, ki se uporabljajo za vsakodnevne družbene dejavnosti. Zagotavlja delovanje gospodarstva v ključnih sektorjih, vključno s finančnim, in krepi delovanje enotnega trga. Z vse večjo digitalizacijo in medsebojno povezanostjo se povečujejo tudi tveganja na področju IKT, zaradi česar je celotna družba – in zlasti finančni sistem – bolj izpostavljena kibernetskim grožnjam ali motnjam IKT. Čeprav so vsesplošna uporaba sistemov IKT ter visoka digitalizacija in povezljivost danes bistvene značilnosti vseh dejavnosti finančnih subjektov v Uniji, digitalna odpornost še ni dovolj vgrajena v njihove operativne okvire.

(2) Uporaba IKT je v zadnjih desetletjih dobila osrednjo vlogo na področju financ in je danes ključnega pomena za delovanje tipičnih dnevnih funkcij vseh finančnih subjektov.

---

* Spremembe: krepki ležeči tisk označuje novo ali spremenjeno besedilo, simbol ▌ pa tiste dele besedila, ki so bili črtani.

[4] [dodati sklic] UL C , , str. .

[5] UL C 155, 30.4.2021, str. 38.

Digitalizacija zajema na primer plačila, ki so se iz gotovinskih in papirnatih metod vse bolj preusmerila v uporabo digitalnih rešitev, ter kliring in poravnave vrednostnih papirjev, elektronsko in algoritemsko trgovanje, operacije posojanja in financiranja, medsebojno financiranje, bonitetne ocene, ▌ obravnavo zahtevkov in operacije zalednih služb. ***Zavarovalniški sektor se je spremenil tudi z uporabo IKT, od pojava digitalnih zavarovalnih posrednikov, ki delujejo z zavarovalniško tehnologijo, do digitalnega zavarovanja in distribucije pogodb.*** Finance so postale večinoma digitalne v celotnem sektorju, poleg tega pa je digitalizacija poglobila medsebojne povezave in odvisnosti znotraj samega finančnega sektorja ter v odnosu do infrastrukture tretjih oseb in tretjih ponudnikov storitev.

(3) Evropski odbor za sistemska tveganja (ESRB) je v poročilu iz leta 2020, ki obravnava sistemska kibernetska tveganja[6], ponovno potrdil, da lahko obstoječa visoka stopnja medsebojne povezanosti finančnih subjektov, finančnih trgov in infrastruktur finančnega trga, zlasti medsebojna odvisnost njihovih sistemov IKT, predstavlja sistemsko ranljivost, saj se lahko lokalni kibernetski incidenti iz katerega koli od približno 22 000 finančnih subjektov[7] v Uniji hitro razširijo na celotni finančni sistem, ne da bi jih pri tem ovirale geografske meje. Resne kršitve na področju IKT, do katerih prihaja v finančnem sektorju, ne vplivajo le na posamezne finančne subjekte. Omogočajo namreč širjenje lokaliziranih ranljivosti po finančnih transmisijskih kanalih in lahko povzročijo škodljive posledice za stabilnost finančnega sistema Unije, saj ustvarjajo upad likvidnosti in splošno izgubo zaupanja v finančne trge.

(4) V zadnjih letih so tveganja na področju IKT pritegnila pozornost nacionalnih, evropskih in mednarodnih oblikovalcev politik, regulativnih organov in organov za določanje standardov, ki si prizadevajo povečati odpornost, določiti standarde ter uskladiti regulativne ali nadzorne naloge. Baselski odbor za bančni nadzor, Odbor za plačila in tržno infrastrukturo, Odbor za finančno stabilnost, Inštitut za finančno stabilnost ter skupine držav G7 in G20 želijo na mednarodni ravni pristojnim organom in upravljavcem trga v različnih jurisdikcijah zagotoviti orodja za krepitev odpornosti njihovih finančnih sistemov. ***Zato je treba tveganje na področju IKT obravnavati v okviru zelo povezanega svetovnega finančnega sistema, v katerem je treba prednostno obravnavati skladnost mednarodne ureditve in sodelovanju med pristojnimi organi na globalni ravni.***

(5) Kljub nacionalnim in evropskim ciljno usmerjenim političnim in zakonodajnim pobudam tveganja na področju IKT še naprej predstavljajo izziv za operativno odpornost, uspešnost in stabilnost finančnega sistema Unije. Reforma, ki je sledila finančni krizi leta 2008, je predvsem okrepila finančno odpornost finančnega sektorja Unije ter si prizadevala zaščititi konkurenčnost in stabilnost Unije z gospodarskega in bonitetnega vidika ter vidika ravnanja na trgu. Čeprav sta varnost IKT in digitalna odpornost del operativnega tveganja, nista bili v ospredju regulativnega programa po

---

[6] Poročilo Evropskega odbora za sistemska tveganja o sistemskih kibernetskih tveganjih, februar 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

[7] Po podatkih iz ocene učinka, ki je priložena reviziji evropskih nadzornih organov (SWD(2017) 308), obstaja približno 5 665 kreditnih institucij, 5 934 investicijskih podjetij, 2 666 zavarovalnic, 1 573 institucij za poklicno pokojninsko zavarovanje, 2 500 družb za upravljanje naložb, 350 tržnih infrastruktur (kot so centralne nasprotne stranke, borze, sistemski internalizatorji, repozitoriji sklenjenih poslov in večstranski sistemi trgovanja), 45 bonitetnih agencij ter 2 500 pooblaščenih plačilnih institucij in institucij za izdajo elektronskega denarja. Skupno je to približno 21 233 subjektov, kar ne vključuje subjektov množičnega financiranja, zakonitih revizorjev in revizijskih podjetij, ponudnikov storitev v zvezi s kriptoimetji in upravljavcev referenčnih vrednosti.

krizi in sta se razvili le na nekaterih področjih politike finančnih storitev in regulativne ureditve Unije ali le v nekaterih državah članicah.

(6) Komisija je v akcijskem načrtu za finančno tehnologijo iz leta 2018[8] poudarila ključno potrebo po večji odpornosti finančnega sektorja Unije tudi z operativnega vidika, da se zagotovi njegova tehnološka varnost in dobro delovanje ter hitro okrevanje po kršitvah in incidentih na področju IKT, kar bi nazadnje omogočilo učinkovito in nemoteno izvajanje finančnih storitev po vsej Uniji, tudi v stresnih situacijah, ter hkrati ohranjalo zaupanje in samozavest potrošnikov in trga.

(7) Evropski bančni organ (EBA), Evropski organ za vrednostne papirje in trge (ESMA) ter Evropski organ za zavarovanja in poklicne pokojnine (EIOPA) (v nadaljnjem besedilu skupaj: evropski nadzorni organi) so aprila 2019 skupaj izdali dva tehnična nasveta, v katerih pozivajo k skladnemu pristopu k tveganjem na področju IKT v finančnem sektorju in priporočajo sorazmerno krepitev digitalne operativne odpornosti industrije finančnih storitev s posebno sektorsko pobudo Unije.

(8) Finančni sektor Unije urejajo harmonizirana enotna pravila, upravlja pa ga evropski sistem finančnega nadzora. Vendar določbe o digitalni operativni odpornosti in varnosti IKT še niso v celoti ali dosledno harmonizirane, čeprav je digitalna operativna odpornost ključnega pomena za zagotavljanje finančne stabilnosti in celovitosti trga v digitalni dobi in nič manj pomembna od na primer skupnih bonitetnih standardov ali standardov ravnanja na trgu. Zato bi bilo treba enotna pravila in sistem nadzora oblikovati tako, da bi vključevala tudi to komponento, in sicer z razširitvijo pooblastil finančnih nadzornikov ***za obvladujejo tveganja na področju IKT v finančnem sektorju,*** za varstvo celovitosti ***in učinkovitosti enotnega*** trga ***ter za spodbujanje njegovega pravilnega delovanja***.

(9) Zakonodajne razlike in neenakomerni nacionalni regulativni ali nadzorni pristopi k tveganjem na področju IKT ovirajo enotni trg finančnih storitev, saj omejujejo nemoteno uveljavljanje pravice do ustanavljanja in opravljanja storitev pri finančnih subjektih s čezmejno prisotnostjo. Prav tako je lahko izkrivljena konkurenca med finančnimi subjekti iste vrste, ki poslujejo v različnih državah članicah. Predvsem na področjih, kjer je harmonizacija s strani Unije zelo omejena – kot na primer pri testiranju digitalne operativne odpornosti – ali pa je sploh ni – kot na primer pri spremljanju tveganj tretjih oseb na področju IKT –, bi lahko razlike, ki izhajajo iz predvidenih sprememb na nacionalni ravni, predstavljale dodatne ovire za delovanje enotnega trga v škodo udeležencem na trgu in finančni stabilnosti.

(10) Določbe, povezane s tveganji na področju IKT, so bile na ravni Unije do zdaj obravnavne le delno, kar povzroča vrzeli ali prekrivanja na pomembnih področjih, kot sta poročanje o incidentih, povezanih z IKT, in testiranje digitalne operativne odpornosti, ter vodi v neskladja zaradi različnih nacionalnih pravil ali stroškovno neučinkovite uporabe prekrivajočih se pravil. To je zlasti škodljivo za intenzivne uporabnike IKT, kot je finančni sektor, saj tehnološka tveganja ne poznajo meja, finančni sektor pa svoje storitve široko uporablja čezmejno znotraj in zunaj Unije.

Posamezni finančni subjekti, ki poslujejo čezmejno ali imajo več dovoljenj (npr. en

[8] Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropski centralni banki, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, z naslovom Akcijski načrt za finančno tehnologijo: za bolj konkurenčen in inovativen evropski finančni sektor, COM(2018)0109, https://ec.europa.eu/info/publications/180308-action-plan-fintech_sl.

finančni subjekt ima lahko dovoljenje za opravljanje bančnih storitev, dovoljenje za investicijsko podjetje in dovoljenje za plačilno institucijo, pri čemer je vsako dovoljenje izdal drug pristojni organ v eni ali več državah članicah), se sami soočajo z operativnimi izzivi pri obravnavanju tveganj na področju IKT in blažitvi škodljivih učinkov incidentov, povezanih z IKT, na skladen in stroškovno učinkovit način.

(10a) Vzpostavitev in vzdrževanje ustreznih infrastruktur omrežja in informacijskega sistema je tudi temeljni pogoj za učinkovito združevanje podatkov o tveganju in prakse poročanja o tveganju, ki sta bistveni zahtevi za preudarno in trajnostno upravljanje tveganj in postopke odločanja kreditnih institucij. Baselski odbor za bančni nadzor je leta 2013 objavil sklop načel za učinkovito združevanje podatkov o tveganju in poročanje o tveganju (BCBS 239) na podlagi dveh splošnih načel upravljanja in infrastrukture IT, ki naj bi se vzpostavila do začetka leta 2016. V skladu s poročilom Evropske centralne banke (ECB) iz maja 2018 o tematskem pregledu o učinkovitem združevanju podatkov o tveganju in poročanju o tveganjih iz maja 2018 ter poročilom o napredku Baselskega odbora za bančni nadzor iz aprila 2020 je bil napredek pri izvajanju, ki so ga dosegle globalne sistemsko pomembne banke, nezadovoljiv in zaskrbljujoč. Da bi olajšala skladnost in usklajevanje z mednarodnimi standardi, bi morala Komisija v tesnem sodelovanju z ECB ter po posvetovanju z Evropskim bančnim organom in Evropskim odborom za sistemska tveganja pripraviti poročilo, v katerem bi ocenila, kako so načela BCBS 239 medsebojno povezana z določbami te uredbe in kako bi jih bilo treba po potrebi vključiti v pravo Unije.

(11) Ker enotnih pravil ni spremljal celovit okvir za tveganja IKT ali operativna tveganja, je potrebna nadaljnja harmonizacija ključnih zahtev glede digitalne operativne odpornosti za vse finančne subjekte. Zmogljivosti in splošna odpornost, ki bi jo finančni subjekti razvili na podlagi takih ključnih zahtev, da bi prenesli prekinitve poslovanja, bi pomagale ohranjati stabilnost in celovitost finančnih trgov Unije in bi tako prispevale k zagotavljanju visoke ravni zaščite vlagateljev in potrošnikov v Uniji. Ker je namen te uredbe prispevati k nemotenemu delovanju enotnega trga, bi morala temeljiti na določbah člena 114 PDEU, kot se razlagajo v skladu z ustaljeno sodno prakso Sodišča Evropske unije.

(12) Cilj te uredbe je najprej utrditi in nadgraditi zahteve glede tveganj na področju IKT, ki so bile doslej obravnavane ločeno v različnih uredbah in direktivah. Ti pravni akti Unije so zajemali glavne kategorije finančnega tveganja (npr. kreditno tveganje, tržno tveganje, kreditno tveganje nasprotne stranke in likvidnostno tveganje, tveganje ravnanja na trgu), vendar v času sprejetja niso mogli celovito obravnavati vseh elementov operativne odpornosti. Zahteve glede operativnih tveganj, ki so bile nadalje razvite v teh pravnih aktih Unije, so pogosto dajale prednost tradicionalnemu kvantitativnemu pristopu k obravnavanju tveganj (zlasti določitev kapitalske zahteve za pokrivanje tveganj na področju IKT), namesto da bi vključevale ciljno usmerjene kvalitativne zahteve za povečanje zmogljivosti z zahtevami, ki bi bile usmerjene v zmogljivosti za zaščito, odkrivanje, omejitev, okrevanje in popravila po incidentih, povezanih z IKT, ali z vzpostavitvijo zmogljivosti za poročanje in digitalno testiranje. Navedene direktive in uredbe naj bi zajemale predvsem bistvena pravila o bonitetnem nadzoru, celovitosti trga ali ravnanju na trgu.

S to pobudo, ki združuje in posodablja pravila o tveganjih na področju IKT, bi bile vse določbe, ki obravnavajo digitalno tveganje v finančnem sektorju, prvič dosledno združene v enem zakonodajnem aktu. Pobuda bi morala tako zapolniti vrzeli ali

odpraviti nedoslednosti v nekaterih pravnih aktih, tudi v zvezi s terminologijo, ki se v njih uporablja, in bi se morala izrecno nanašati na tveganja na področju IKT s ciljno usmerjenimi pravili o zmožnostih upravljanja tveganj na področju IKT, poročanju in testiranju ter spremljanju tveganj tretjih oseb. ***Namen te pobude je tudi okrepiti ozaveščenost o tveganjih na področju IKT, pri čemer priznava, da bi lahko incidenti na področju IKT in pomanjkanje operativne odpornosti ogrozili finančno trdnost finančnih subjektov.***

(13) Finančni subjekti bi morali pri obravnavanju tveganj na področju IKT slediti istemu pristopu in upoštevati ista na načelih temelječa pravila ***v skladu z njihovo velikostjo, naravno, kompleksnostjo in profilom***. Doslednost prispeva k povečanju zaupanja v finančni sistem in ohranjanju njegove stabilnosti, zlasti v primerih ***visoke odvisnosti od*** sistemov, platform in infrastruktur IKT, ki prinašajo tudi povečano digitalno tveganje.

S spoštovanjem osnovne kibernetske higiene bi se tudi preprečilo nastajanje znatnih stroškov za gospodarstvo, saj bi se na najmanjšo možno mero zmanjšali učinki in znižali stroški motenj na področju IKT.

(14) Uporaba uredbe pomaga zmanjšati regulativno zapletenost, spodbuja konvergenco nadzora, povečuje pravno varnost ter hkrati prispeva k omejevanju stroškov izpolnjevanja obveznosti, zlasti za čezmejne finančne subjekte, in k zmanjšanju izkrivljanja konkurence. Zato se zdi, da je izbira uredbe za vzpostavitev skupnega okvira za digitalno operativno odpornost finančnih subjektov najustreznejši način za zagotovitev homogene in skladne uporabe vseh komponent upravljanja tveganj na področju IKT v finančnem sektorju Unije.

(14a) Vendar izvajanje te uredbe ne bi smelo ovirati inovacij v zvezi s tem, kako finančni subjekti obravnavajo vprašanja digitalne operativne odpornosti ob upoštevanju njenih določb, niti v zvezi s storitvami, ki jih ponujajo, ali storitvami, ki jih ponujajo tretji ponudniki storitev IKT.

(15) Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta[9] je poleg zakonodaje o finančnih storitvah trenutni splošni okvir za kibernetsko varnosti na ravni Unije. Med sedmimi ključnimi sektorji se navedena direktiva uporablja tudi za tri vrste finančnih subjektov, in sicer za kreditne institucije, mesta trgovanja in centralne nasprotne stranke. Vendar Direktiva (EU) 2016/1148 določa mehanizem identifikacije izvajalcev bistvenih storitev na nacionalni ravni, zato so v praksi le nekatere kreditne institucije, mesta trgovanja in centralne nasprotne stranke, ki jih opredelijo države članice, zajete v njeno področje uporabe in morajo izpolnjevati zahteve glede varnosti IKT in obveščanja o incidentih, določene v njej.

(16) Ta uredba dviguje raven harmonizacije komponent digitalne odpornosti z uvedbo zahtev glede upravljanja tveganj na področju IKT in poročanja o incidentih, povezanih z IKT, ki so strožje od tistih, ki jih določa veljavna zakonodaja Unije o finančnih storitvah, zato je tudi harmonizacija večja v primerjavi z zahtevami iz Direktive (EU) 2016/1148. Posledično je ta uredba ***za finančne subjekte*** lex specialis glede na Direktivo (EU) 2016/1148.

Ključno je, da se ohrani močna povezava med finančnim sektorjem in horizontalnim okvirom kibernetske varnosti Unije, kar bi zagotovilo skladnost s strategijami

[9] Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016, str. 1).

kibernetske varnosti, ki so jih države članice že sprejele, in finančnim nadzornikom omogočilo, da se seznanijo s kibernetskimi incidenti, ki prizadenejo druge sektorje, zajete v Direktivi (EU) 2016/1148.

(17) Finančni subjekti iz Direktive (EU) 2016/1148 bi morali ostati del „ekosistema“ navedene direktive (npr. skupina za sodelovanje na področju varnosti omrežij in informacij ter skupine za odzivanje na incidente na področju računalniške varnosti), da bi se omogočil medsektorski učni proces in učinkovito črpalo iz izkušenj drugih sektorjev pri obravnavanju kibernetskih groženj.

Evropski nadzorni organi oziroma pristojni nacionalni organi bi morali imeti možnost sodelovati v razpravah o strateških politikah oziroma tehničnem delu skupine za sodelovanje na področju varnosti omrežij in informacij, si izmenjevati informacije oziroma nadalje sodelovati z enotnimi kontaktnimi točkami, določenimi v skladu z Direktivo (EU) 2016/1148. ***Skupni nadzorni organ, glavni nadzornik in*** pristojni organi iz te uredbe bi se morali tudi posvetovati in sodelovati z nacionalnimi skupinami za odzivanje na incidente na področju računalniške varnosti, določenimi v skladu s členom 9 Direktive (EU) 2016/1148.

Poleg tega bi morala ta uredba zagotoviti, da se mreži skupin CSIRT, vzpostavljeni z Direktivo (EU) 2016/1148, zagotovijo podrobnosti o večjih incidentih, povezanih z IKT.

(18) Prav tako je pomembno zagotoviti skladnost z direktivo o evropski kritični infrastrukturi, ki se trenutno pregleduje, da bi se povečali zaščita in odpornost kritične infrastrukture proti grožnjam, ki niso povezane s kibernetsko varnostjo, ***in z direktivo o odpornosti kritičnih subjektov***[10], kar bi lahko imelo posledice za finančni sektor.

(19) Ponudniki storitev računalništva v oblaku so ena od kategorij ponudnikov digitalnih storitev, ki jih zajema Direktiva (EU) 2016/1148. Kot taki so predmet naknadnega nadzora, ki ga izvajajo nacionalni organi, imenovani v skladu z navedeno direktivo, in ki je omejen na zahteve glede varnosti IKT in obveščanja o incidentih, določene v navedenem aktu. Ker okvir nadzora, vzpostavljen s to uredbo, velja za vse ključne tretje ponudnike storitev IKT, vključno s ponudniki storitev računalništva v oblaku, kadar zagotavljajo storitve IKT finančnim subjektom, bi ga bilo treba obravnavati kot dopolnitev nadzora, ki se izvaja v skladu z Direktivo (EU) 2016/1148***, tako vsebinske kot postopkovne zahteve, ki veljajo za ključne tretje ponudnike storitev IKT iz te uredbe, pa bi morale biti koherentne in usklajene z zahtevami, ki se uporabljajo v skladu z navedeno direktivo.*** Poleg tega bi moral okvir nadzora, vzpostavljen s to uredbo, zajemati ponudnike storitev računalništva v oblaku, saj ni horizontalnega nesektorskega okvira Unije, ki bi vzpostavljal organ za digitalni nadzor.

(20) Za ohranitev popolnega nadzora nad tveganji na področju IKT morajo finančni subjekti imeti celovite zmogljivosti, ki omogočajo močno in učinkovito upravljanje tveganj na področju IKT, skupaj s posebnimi mehanizmi in politikami za poročanje o incidentih, povezanih z IKT, testiranje sistemov, kontrol in postopkov IKT ter upravljanje tveganj tretjih oseb in znotraj skupine na področju IKT. Raven digitalne operativne odpornosti finančnega sistema je treba dvigniti ter hkrati omogočiti sorazmerno uporabo zahtev ***ob upoštevanju njihove narave, obsega, kompleksnosti in splošnega profila tveganja***.

[10] Direktiva Sveta 2008/114/ES z dne 8. decembra 2008 o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe po izboljšanju njene zaščite (UL L 345, 23.12.2008, str. 75).

(21) Pragovi in taksonomije poročanja o incidentih, povezanih z IKT, se na nacionalni ravni zelo razlikujejo. Z ustreznim delom Agencije Evropske unije za kibernetsko varnost (ENISA)[11] in skupine za sodelovanje na področju varnosti omrežij in informacij je mogoče doseči skupno podlago za finančne subjekte iz Direktive (EU) 2016/1148, vendar za preostale finančne subjekte še vedno obstajajo ali se lahko pojavijo različni pristopi glede pragov in taksonomij. To vključuje številne zahteve, ki jih morajo spoštovati finančni subjekti, zlasti kadar poslujejo v različnih jurisdikcijah v Uniji in kadar so del finančne skupine. Poleg tega lahko te razlike ovirajo vzpostavitev nadaljnjih enotnih ali centraliziranih mehanizmov Unije, ki pospešujejo postopek poročanja in podpirajo hitro in nemoteno izmenjavo informacij med pristojnimi organi, kar je bistvenega pomena za obravnavo tveganj na področju IKT v primeru obsežnih napadov s potencialno sistemskimi posledicami.

(21a) Da bi zmanjšali upravno breme ter preprečili zapletenost in podvajanje zahtev glede poročanja za ponudnike plačilnih storitev, ki spadajo na področje uporabe te uredbe, se zahteve glede poročanja o incidentih iz Direktive (EU) 2015/2366 ne bi smele več uporabljati. Kreditne institucije, institucije za izdajo elektronskega denarja in plačilne institucije bi morale kot take v skladu s to uredbo poročati o vseh operativnih incidentih ali incidentih, povezanih s plačili ali plačili, ki niso povezani s plačili, o katerih se je predhodno poročalo na podlagi Direktive (EU) 2015/2366, ne glede na to, ali so incidenti povezani z IKT ali ne.

(22) Določiti je treba pravila za ***vzpostavitev trdne*** ureditve poročanja o incidentih, povezanih z IKT, z zahtevami ***za odpravo vrzeli*** v zakonodaji ***sektorja finančnih storitev*** ter morebitnih prekrivanj in podvajanj za znižanje stroškov, da lahko pristojni organi izpolnjujejo svoje nadzorne vloge s pridobitvijo celovitega vpogleda v naravo, pogostost, pomen in učinek incidentov, povezanih z IKT, ter da se okrepi izmenjava informacij med ustreznimi javnimi organi, vključno z organi kazenskega pregona in organi za reševanje. Zato je treba nujno uskladiti ureditev poročanja o incidentih, povezanih z IKT, tako da se od vseh finančnih subjektov zahteva, naj poročajo le svojim pristojnim organom ***v okviru usklajenega mehanizma iz te uredbe***. Poleg tega bi morali biti evropski nadzorni organi pooblaščeni za nadaljnjo opredelitev elementov poročanja o incidentih, povezanih z IKT, kot so taksonomija, časovni okviri, nabori podatkov, predloge in veljavni pragovi.

(23) Zahteve glede testiranja digitalne operativne odpornosti so se v nekaterih finančnih podsektorjih razvile v različnih in ***včasih*** neusklajenih nacionalnih okvirih, ki ista vprašanja obravnavajo na različne načine. To vodi do podvajanja stroškov za čezmejne finančne subjekte in ***lahko ovira*** vzajemno priznavanje rezultatov. Neusklajeno testiranje lahko torej razdeli enotni trg.

(24) Poleg tega ranljivosti ostajajo neodkrite, kadar se testiranje ne zahteva, zaradi česar so finančni subjekt ter nazadnje stabilnost in integriteta finančnega sektorja izpostavljeni večjemu tveganju. Brez posredovanja Unije bi bilo testiranje digitalne operativne odpornosti še naprej neenotno in ne bi bilo vzajemnega priznavanja rezultatov testiranja v različnih jurisdikcijah. Ker je malo verjetno, da bi drugi finančni podsektorji sprejeli take sheme v večjem obsegu, bi bili prikrajšani za potencialne koristi, kot so razkrivanje ranljivosti in tveganj, testiranje obrambnih zmogljivosti in neprekinjenega poslovanja

[11] Razvrščanje incidentov na podlagi referenčne taksonomije agencije ENISA, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

ter večje zaupanje strank, dobaviteljev in poslovnih partnerjev. Za odpravo takih prekrivanj, razhajanj in vrzeli je treba določiti pravila za usklajeno testiranje s strani finančnih subjektov in pristojnih organov, s čimer bi se omogočilo vzajemno priznavanje naprednega testiranja za pomembne finančne subjekte.

(25) Odvisnost finančnih subjektov od storitev IKT deloma temelji na njihovi potrebi po prilagajanju nastajajočemu konkurenčnemu digitalnemu svetovnemu gospodarstvu, povečanju njihove poslovne učinkovitosti in zadostitvi povpraševanju potrošnikov. Narava in obseg te odvisnosti se v zadnjih letih nenehno spreminjata ter sta gonilni sili pri zniževanju stroškov v finančnem posredništvu, širjenju poslovanja in nadgradljivosti ob uvajanju finančnih dejavnosti, hkrati pa zagotavljata široko paleto orodij IKT za upravljanje zapletenih notranjih postopkov.

(26) To obsežno uporabo storitev IKT dokazujejo zapleteni pogodbeni dogovori, pri katerih se finančni subjekti pogosto srečujejo s težavami pri pogajanjih o pogodbenih pogojih, ki so prilagojeni bonitetnim standardom ali drugim regulativnim zahtevam, ki zavezujejo subjekte, ali sicer pri uveljavljanju posebnih pravic, kot so pravice do dostopa ali revizije, če so slednje vključene v dogovore. Poleg tega veliko takih pogodb ne zagotavlja zadostnih zaščitnih ukrepov, ki bi omogočali celovito spremljanje postopkov oddaje naročil podizvajalcem, zaradi česar finančni subjekt ne more oceniti teh povezanih tveganj. Nadalje, ker tretji ponudniki storitev IKT pogosto zagotavljajo standardizirane storitve različnim vrstam strank, take pogodbe morda ne bodo vedno ustrezno zadovoljile posameznih ali posebnih potreb akterjev v finančnem sektorju.

(27) Kljub nekaterim splošnim pravilom o zunanjem izvajanju v nekaterih zakonodajnih aktih Unije o finančnih storitvah nadzor nad pogodbeno razsežnostjo ni v celoti vključen v zakonodajo Unije. Ker ni jasnih in prilagojenih standardov Unije, ki bi veljali za pogodbene dogovore, sklenjene s tretjimi ponudniki storitev IKT, zunanji vir tveganj na področju IKT ni celovito obravnavan. Zato je treba določiti nekatera ključna načela, ki bodo finančnim subjektom zagotovila usmeritve pri upravljanju tveganj tretjih oseb na področju IKT, skupaj s sklopom temeljnih pogodbenih pravic v zvezi z različnimi elementi izvajanja in odpovedi pogodb, in sicer z namenom vključitve nekaterih minimalnih zaščitnih ukrepov, ki krepijo zmožnost finančnih subjektov, da učinkovito spremljajo vsa tveganja na ravni tretjih oseb na področju IKT.

(28) Trenutno ni homogenosti in konvergence v zvezi s tveganji tretjih oseb na področju IKT in odvisnostjo od tretjih oseb na področju IKT Kljub nekaterim prizadevanjem za obravnavo področja zunanjega izvajanja, kot so priporočila iz leta 2017 o oddajanju v zunanje izvajanje ponudnikom storitev v oblaku[12], je vprašanje sistemskega tveganja, ki bi ga lahko povzročila izpostavljenost finančnega sektorja omejenemu številu ključnih tretjih ponudnikov storitev IKT, v zakonodaji Unije komajda obravnavano. To pomanjkanje na ravni Unije dodatno stopnjuje neobstoj posebnih pooblastil in orodij, ki bi nacionalnim nadzornikom omogočala dobro razumevanje odvisnosti od tretjih oseb na področju IKT in ustrezno spremljanje tveganj, ki izhajajo iz koncentracije takih odvisnosti od tretjih oseb na področju IKT.

(29) Ob upoštevanju možnih sistemskih tveganj, ki jih prinašajo povečano oddajanje del v zunanje izvajanje in koncentracija odvisnosti od tretjih oseb na področju IKT, ter ob upoštevanju nezadostnosti nacionalnih mehanizmov, ki bi finančnim nadzornikom

[12] Priporočila o oddajanju v zunanje izvajanje ponudnikom storitev v oblaku (EBA/REC/2017/03), zdaj razveljavljena s smernicami EBA o zunanjem izvajanju (EBA/GL/2019/02).

omogočali kakovostno in količinsko opredelitev ter odpravo posledic tveganj na področju IKT, ki se pojavljajo pri ključnih tretjih ponudnikih storitev IKT, je treba vzpostaviti ustrezen okvir nadzora Unije, ki omogoča stalno spremljanje dejavnosti tretjih ponudnikov storitev IKT, ki ***finančnim subjektom ponujajo kritične storitve***. ***Ker z zagotavljanjem storitev IKT znotraj skupine niso povezana enaka tveganja, ponudniki storitev IKT, ki so del iste skupine ali institucionalne jamstvene sheme, ne bi smeli biti opredeljeni kot ključni tretji ponudniki storitev IKT.***

(30) Ker so grožnje na področju IKT vse bolj zapletene in izpopolnjene, so dobri ukrepi za odkrivanje in preprečevanje večinoma odvisni od redne izmenjave obveščevalnih podatkov o grožnjah in ranljivostih med finančnimi subjekti. Izmenjava informacij prispeva k večji ozaveščenosti o kibernetskih grožnjah, kar posledično krepi sposobnost finančnih subjektov za preprečevanje, da bi se grožnje spremenile v dejanske incidente, in finančnim subjektom omogoča, da bolje omejijo učinke incidentov, povezanih z IKT, in si učinkoviteje opomorejo. Videti je, da je ob odsotnosti smernic na ravni Unije več dejavnikov oviralo tako izmenjavo obveščevalnih podatkov, zlasti negotovost glede združljivosti s pravili o varstvu podatkov, omejevalnih ravnanjih in odgovornosti. ***Zato je pomembno okrepiti dogovore o sodelovanju in poročanje med finančnimi subjekti in pristojnimi organi ter izmenjavo informacij z javnostjo, da bi razvili odprt okvir za izmenjavo obveščevalnih podatkov in pristop na podlagi „vgrajene varnosti“, ki sta bistvena za okrepitev operativne odpornosti in pripravljenosti finančnega sektorja na tveganja na področju IKT. Dogovori o izmenjavi informacij bi morali dosledno ustrezno upoštevati morebitna tveganja, povezana s kibernetsko varnostjo, varstvom podatkov ali poslovno zaupnostjo.***

(31) Poleg tega se koristne informacije prikrivajo zaradi pomislekov glede vrste informacij, ki se lahko delijo z drugimi udeleženci na trgu ali nenadzornimi organi (kot je ENISA za analitični prispevek ali Europol za namene kazenskega pregona). Obseg in kakovost izmenjave informacij ostajata omejena in razdrobljena, pri čemer se ustrezne izmenjave izvajajo večinoma lokalno (z nacionalnimi pobudami) in brez doslednih dogovorov o izmenjavi informacij na ravni Unije, ki bi bili prilagojeni potrebam integriranega finančnega sektorja. ***Zato je treba v celotnem nadzornem ciklu te komunikacijske kanale okrepiti, k temu pa morajo prispevati nadzorni organi, kadar je to potrebno in ustrezno.***

(32) Finančne subjekte bi bilo treba ***tudi*** spodbuditi, da skupaj izkoristijo svoje individualno znanje in praktične izkušnje na strateški, taktični in operativni ravni, da bi tako okrepili svoje zmogljivosti za ustrezno ocenjevanje in spremljanje kibernetskih groženj, zaščito pred njimi in odzivanje nanje. Zato je treba omogočiti, da se na ravni Unije vzpostavijo mehanizmi za prostovoljne dogovore o izmenjavi informacij, ki bi, kadar bi se izvajali v zaupanja vrednih okoljih, finančni skupnosti pomagali, da preprečuje grožnje in se skupaj odziva nanje s hitrim omejevanjem širjenja tveganj na področju IKT in preprečevanjem širjenja morebitnih negativnih učinkov po finančnih kanalih. Navedene mehanizme bi bilo treba izvajati v popolni skladnosti z veljavnimi pravili Unije s področja konkurenčnega prava[13] in na način, ki zagotavlja popolno spoštovanje pravil Unije o varstvu podatkov, zlasti Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta[14], predvsem kadar je obdelava osebnih podatkov potrebna za namene zakonitega

[13] Sporočilo Komisije – Smernice o uporabi člena 101 Pogodbe o delovanju Evropske unije za sporazume o horizontalnem sodelovanju, 2011/C 11/01.

[14] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri

interesa, za katerega si prizadeva upravljavec ali tretja oseba, kot je navedeno v točki (f) člena 6(1) navedene uredbe.

(33) Ne glede na široko pokritost, ki jo predvideva ta uredba, bi bilo treba pri uporabi pravil o digitalni operativni odpornosti***, vključno pri izvajanju zahtev iz okvira za upravljanje tveganj,*** upoštevati pomembne razlike med finančnimi subjekti glede njihove velikosti, ***narave, kompleksnosti in profila tveganja***. Načeloma bi morali finančni subjekti pri usmerjanju virov in zmogljivosti k izvajanju okvira za upravljanje tveganj na področju IKT najti ustrezno ravnotežje med svojimi potrebami v zvezi z IKT ter svojo velikostjo, ***naravo, kompleksnostjo,*** poslovnim profilom ***in profilom relativnega tveganja***, pristojni organi pa bi morali še naprej ocenjevati in pregledovati pristop takega razdeljevanja.

(34) Ker imajo večji finančni subjekti morda precejšnje vire in bi jih lahko hitro uporabili za razvoj struktur upravljanja in oblikovanje različnih poslovnih strategij, bi se moralo le od finančnih subjektov, ki niso mikro podjetja v smislu te uredbe, zahtevati, naj vzpostavijo bolj zapletene ureditve upravljanja. Taki subjekti so zlasti bolje opremljeni, da vzpostavijo namenske funkcije upravljanja za nadziranje dogovorov s tretjimi ponudniki storitev IKT ali obvladovanje kriz, organizirajo upravljanje tveganj na področju IKT v skladu z modelom treh obrambnih linij ali sprejmejo dokument o človeških virih, ki izčrpno pojasnjuje politike v zvezi s pravicami do dostopa.

Prav tako bi bilo treba le take finančne subjekte pozvati, da izvajajo poglobljene ocene po večjih spremembah infrastruktur in procesov omrežja ter informacijskega sistema, redno izvajajo analize tveganj za obstoječe sisteme IKT ali razširijo testiranje neprekinjenega poslovanja ter načrtov odzivanja in okrevanja po katastrofi, da zajamejo scenarije preklopa med primarno infrastrukturo IKT in redundantnimi obrati.

(35) Ker bi morali penetracijsko testiranje na podlagi analize groženj izvajati le finančni subjekti, ki so bili opredeljeni kot pomembni za namene naprednega testiranja digitalne odpornosti, bi bilo treba upravne postopke in finančne stroške, povezane z izvajanjem takih testov, prenesti na majhen delež finančnih subjektov. Nazadnje, da bi se zmanjšala regulativna bremena, bi se moralo le od finančnih subjektov, ki niso mikro podjetja, zahtevati, da redno poročajo pristojnim organom o vseh ***predvidenih*** stroških in izgubah, ki so nastali zaradi ***znatnih*** motenj na področju IKT, ***večjih incidentih, povezanih z IKT,*** in rezultatih pregledov po ***teh incidentih***, ki se izvedejo po večjih motnjah IKT.

(36) Upravljalni organ bi moral ohraniti ključno in aktivno vlogo pri usmerjanju in prilagajanju okvira za upravljanje tveganj na področju IKT in splošne strategije za digitalno odpornost, da se zagotovi popolna prilagoditev in splošna skladnost med poslovnimi strategijami finančnih subjektov na eni strani in upravljanjem tveganj na področju IKT na drugi strani. Pristop upravljalnega organa se ne bi smel osredotočati le na sredstva za zagotavljanje odpornosti sistemov IKT, temveč bi moral v sklopu politik, ki na vsaki ravni podjetja in pri vseh zaposlenih vzbuja močan občutek ozaveščenosti glede kibernetskih tveganj in zavezanost spoštovanju stroge kibernetske higiene na vseh ravneh, vključevati tudi ljudi in postopke.

Končna odgovornost upravljalnega organa pri upravljanju tveganj finančnega subjekta

---

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).

na področju IKT bi morala biti poglavitno načelo navedenega celovitega pristopa, ki se nadalje prenese v stalno sodelovanje upravljalnega organa pri nadzoru spremljanja upravljanja tveganj na področju IKT.

(37) Poleg tega je polna odgovornost upravljalnega organa povezana z zagotavljanjem zadostnih naložb v IKT in skupnega proračuna, da lahko finančni subjekt doseže minimalne zahteve glede digitalne operativne odpornosti.

(38) Ta uredba črpa navdih iz ustreznih mednarodnih, nacionalnih in panožnih standardov, smernic, priporočil ali pristopov k upravljanju kibernetskih tveganj[15] in spodbuja vrsto funkcij, ki omogočajo splošno ureditev upravljanja tveganj na področju IKT. Dokler glavne zmogljivosti, ki jih vzpostavijo finančni subjekti, ustrezajo potrebam ciljev, predvidenih s funkcijami (prepoznavanje, zaščita in preprečevanje, odkrivanje, odzivanje in okrevanje, učenje in razvoj ter komunikacija), določenimi v tej uredbi, lahko finančni subjekti uporabljajo modele upravljanja tveganj na področju IKT, ki so različno oblikovani ali kategorizirani.

(39) Da bi finančni subjekti lahko sledili razvijajočemu se področju kibernetskih groženj, bi morali vzdrževati posodobljene sisteme IKT, ki so zanesljivi in imajo zadostno zmogljivost ne le za zagotavljanje obdelave podatkov, ki je potrebna za izvajanje njihovih storitev, temveč tudi za zagotavljanje tehnološke odpornosti, ki finančnim subjektom omogoča, da se ustrezno spopadajo z dodatnimi obdelovalnimi potrebami, ki jih lahko povzročijo zaostrene tržne ali druge neugodne razmere. Ta uredba sicer ne vključuje standardizacije posebnih sistemov, orodij ali tehnologij IKT, vendar temelji na ustrezni uporabi evropskih in mednarodno priznanih tehničnih standardov (npr. ISO) ali dobrih panožnih praks s strani finančnih subjektov, če je taka uporaba v celoti skladna s posebnimi nadzorniškimi navodili za uporabo in vključitev mednarodnih standardov.

(40) Učinkoviti načrti neprekinjenega poslovanja in vnovične vzpostavitve delovanja morajo finančnim subjektom omogočiti takojšnje in hitro reševanje incidentov, povezanih z IKT, zlasti kibernetskih napadov, z omejevanjem škode in dajanjem prednosti nadaljevanju dejavnosti in ukrepom za ponovno vzpostavitev delovanja***, pri tem pa upoštevati, ali gre za kritično ali pomembno funkcijo***. Čeprav bi morali sistemi za varnostno kopiranje začeti delovati brez nepotrebnega odlašanja, tak zagon nikakor ne bi smel ogroziti celovitosti in varnosti omrežja in informacijskih sistemov ali zaupnosti podatkov.

(41) Ta uredba finančnim subjektom omogoča, da prilagodljivo določijo cilje glede časa za obnovitev in posledično določijo take cilje ob popolnem upoštevanju narave in kritičnosti zadevne funkcije ter morebitnih posebnih poslovnih potreb, vendar bi se morala pri določanju takih ciljev zahtevati tudi ocena možnega splošnega vpliva na učinkovitost trga.

(42) Pomembne posledice kibernetskih napadov se razširijo, ko se zgodijo v finančnem

[15]CPMI-IOSCO, Guidance on cyber resilience for financial market infrastructures (Smernice o kibernetski odpornosti za infrastrukture finančnih trgov), https://www.bis.org/cpmi/publ/d146.pdf; G7, Fundamental Elements of Cybersecurity for the Financial Sector (Temeljni elementi kibernetske varnosti za finančni sektor), https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; Okvir inštituta NIST za kibernetsko varnost, https://www.nist.gov/cyberframework; FSB, Komplet orodij za odziv na kibernetske incidente in odpravo posledic, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document.

sektorju, za katerega obstaja veliko večje tveganje, da bo tarča zlonamernih razširjevalcev, ki iščejo finančne koristi neposredno pri viru. Da bi se omejila taka tveganja in preprečila izguba integritete sistemov IKT ali njihova nedostopnost ter poseganje v zaupne podatke ali utrpela škoda na fizični infrastrukturi IKT, bi bilo treba znatno izboljšati poročanje finančnih subjektov o večjih incidentih, povezanih z IKT.

Poročanje o incidentih, povezanih z IKT, bi bilo treba uskladiti tako, da bi se od vseh finančnih subjektov zahtevalo, da poročajo le svojim pristojnim organom. To poročanje bi veljalo za vse finančne subjekte, vendar ne bi smelo na vse vplivati enako, saj bi bilo treba določiti ustrezne pragove pomembnosti in časovne okvire tako, da bi se zajeli le večji incidenti, povezani z IKT. Neposredno poročanje bi finančnim nadzornikom omogočilo dostop do informacij o incidentih, povezanih z IKT. Kljub temu bi morali finančni nadzorniki te informacije posredovati nefinančnim javnim organom (pristojni organi na področju varnosti omrežij in informacij, nacionalni organi za varstvo podatkov in organi kazenskega pregona v primeru incidentov, ki vključujejo kaznivo dejanje). Informacije o incidentih, povezanih z IKT, bi bilo treba vzajemno usmerjati: finančni nadzorniki bi morali finančnemu subjektu zagotoviti vse potrebne povratne informacije ali smernice, evropski nadzorni organi pa bi morali deliti anonimizirane podatke o grožnjah in ranljivostih v zvezi z dogodkom, da bi pripomogli k širši kolektivni obrambi.

(43) Predvideti bi bilo treba nadaljnji razmislek o morebitni centralizaciji poročil o incidentih, povezanih z IKT, in sicer z enotnim vozliščem EU ***za poročanje o večjih incidentih, povezanih z IKT***, ki bi neposredno prejemalo ustrezna poročila in samodejno obveščalo nacionalne pristojne organe ali pa zgolj centraliziralo poročila, ki jih pošljejo nacionalni pristojni organi, in izpolnjevalo usklajevalno vlogo. Evropski nadzorni organi bi morali v posvetovanju z ECB in ENISA do določenega datuma pripraviti skupno poročilo, v katerem bi preučili izvedljivost vzpostavitve takega vozlišča EU.

(44) Finančni subjekti***, ki niso mikro podjetja,*** bi morali redno testirati svoje sisteme IKT in zaposlene v zvezi z učinkovitostjo njihovih sposobnosti preprečevanja, odkrivanja, odzivanja in okrevanja za odkrivanje in odpravo morebitnih ranljivosti na področju IKT, da bi se dosegla trdna digitalna operativna odpornost, ki je skladna z mednarodnimi standardi (kot so temeljni elementi za penetracijsko testiranje na podlagi analize groženj skupine G7). Testiranje bi moralo vključevati široko paleto orodij in ukrepov, od ocene osnovnih zahtev (npr. ocene in pregledi ranljivosti, analize prosto dostopnih virov, ocene varnosti omrežja, analize vrzeli, pregledi fizične varnosti, vprašalniki in rešitve programske opreme za pregledovanje, pregledi izvorne kode, kjer je to mogoče, testiranja na podlagi scenarijev, testiranje združljivosti, testiranje učinkovitosti ali celovito testiranje) do naprednejših testov (npr. penetracijsko testiranje na podlagi analize groženj za tiste finančne subjekte, ki so z vidika IKT dovolj pripravljeni na izvajanje takih testov), da bi se bilo mogoče odzvati na razlike med finančnimi podsektorji in znotraj njih glede pripravljenosti finančnih subjektov na področju kibernetske varnosti. Testiranje digitalne operativne odpornosti bi zato moralo biti zahtevnejše za pomembne finančne subjekte (kot so velike kreditne institucije, borze vrednostnih papirjev, centralne depotne družbe, centralne nasprotne stranke itd.). Hkrati bi moralo biti testiranje digitalne operativne odpornosti pomembnejše za nekatere podsektorje, ki imajo osrednjo sistemsko vlogo (npr. plačila, bančništvo, kliring in poravnava), in manj pomembno za druge podsektorje (npr. upravljavci premoženja, bonitetne agencije itd.). Čezmejni finančni subjekti, ki uveljavljajo pravico do

ustanavljanja ali opravljanja storitev v Uniji, bi morali v svoji matični državi članici izpolniti enoten sklop zahtev za napredno testiranje (npr. penetracijsko testiranje na podlagi analize groženj), pri čemer bi moralo testiranje vključevati infrastrukture IKT v vseh jurisdikcijah, kjer čezmejna skupina deluje znotraj Unije, da bi imele čezmejne skupine stroške testiranja le v eni jurisdikciji. ***Poleg tega bi si morali Komisija in pristojni organi za okrepitev sodelovanja z zaupanja vrednimi tretjimi državami na področju odpornosti finančnih subjektov prizadevati za vzpostavitev okvira za vzajemno priznavanje rezultatov penetracijskega testiranja na podlagi analize groženj.***

Države članice bi morale imenovati en sam javni organ, ki bi bil na nacionalni ravni odgovoren za penetracijsko testiranje na podlagi analize groženj v finančnem sektorju. Enotni javni organ je lahko med drugim pristojni nacionalni organ ali javni organ, imenovan v skladu s členom 8 Direktive (EU) 2016/1148. Enotni javni organ bi moral biti odgovoren za izdajo potrdil, da je bilo penetracijsko testiranje na podlagi analize groženji zvedeno v skladu z zahtevami. Takšna potrdila bi morala olajšati vzajemno priznavanje testiranja med pristojnimi organi.

Nekateri finančni subjekti lahko izvajajo notranje napredno testiranje, drugi pa bodo najeli zunanje preizkuševalce iz Unije ali iz tretje države. Zato je pomembno, da za vse preizkuševalce veljajo enake jasne zahteve, za zagotovitev neodvisnosti notranjih preskuševalcev pa bi morali njihovo uporabo odobriti pristojni organi.

Metodologija za penetracijsko testiranje na podlagi analize groženj ne bi smela biti obvezna, vendar bi bilo treba uporabo obstoječega okvira TIBER-EU šteti za skladno z zahtevami penetracijskega testiranja na podlagi analize groženj iz te uredbe.

Finančni subjekti bi morali do začetka veljavnosti te uredbe ter razvoja in sprejetja pooblaščenih regulativnih tehničnih standardov v zvezi s penetracijskim testiranjem na podlagi analize groženj s strani evropskih nadzornih organov upoštevati ustrezne smernice in okvire Unije, ki se uporabljajo za penetracijsko testiranje na podlagi obveščevalnih podatkov, saj se bodo ti uporabljali tudi po začetku veljavnosti te uredbe.

(44a) Za izvajanje penetracijskega testiranja na podlagi analize groženj – in za upravljanje kibernetske varnosti na splošno ter preprečevanje kibernetskih napadov – bi moral biti v celoti odgovoren finančni subjekt, potrdila, ki jih predložijo organi, pa bi morala biti namenjena izključno vzajemnemu priznavanju in ne bi smela preprečevati nadaljnjega ukrepanja na ravni tveganja na področju IKT, ki mu je izpostavljen finančni subjekt, niti se ne bi smela obravnavati kot potrditev njegovih zmogljivosti za obvladovanje in zmanjševanje tveganj na področju IKT.

(45) Da bi se zagotovilo učinkovito spremljanje tveganj tretjih oseb na področju IKT, je treba določiti sklop na načelih temelječih pravil, ki bodo finančnim subjektom zagotavljala usmeritve pri spremljanju tveganj, ki izhajajo iz oddajanja funkcij v zunanje izvajanje tretjim ponudnikom storitev IKT, ***zlasti v zvezi z zagotavljanjem kritičnih ali pomembnih funkcij, ki jih zagotavlja ključni tretji ponudnik storitev IKT,*** in, splošneje, iz odvisnosti od tretjih oseb na področju IKT.

(46) Finančni subjekt bi moral biti ves čas v celoti odgovoren za izpolnjevanje obveznosti iz te uredbe. Organizirati bi bilo treba sorazmerno spremljanje tveganj, ki se pojavljajo na ravni tretjega ponudnika storitev IKT, z ustrezno preučitvijo obsega, zapletenosti in pomena odvisnosti, povezanih z IKT, kritičnosti ali pomena storitev, postopkov ali

funkcij, za katere veljajo pogodbeni dogovori, in nazadnje na podlagi natančne ocene morebitnega vpliva na kontinuiteto in kakovost finančnih storitev na ravni posameznika in skupine, kot je ustrezno***, in ali storitve IKT zagotavljajo ponudniki storitev znotraj skupine ali tretji ponudniki storitev***.

(47) Izvajanje takega spremljanja bi moralo slediti strateškemu pristopu k tveganjem tretjih oseb na področju IKT, ki je bil formaliziran s sprejetjem posebne strategije s strani upravljalnega organa finančnega subjekta, in temeljiti na nenehnem preverjanju vseh takih odvisnosti od tretjih oseb na področju IKT. Finančni nadzorniki bi morali redno prejemati bistvene informacije iz registrov in imeti možnost, da na ad hoc podlagi zahtevajo izpiske iz njih, da se poveča ozaveščenost nadzornikov o odvisnosti od tretjih oseb na področju IKT in nadalje podpre okvir nadzora, vzpostavljen s to uredbo.

(48) Temeljita analiza pred sklenitvijo pogodbe bi se morala opraviti pred uradno sklenitvijo pogodbenih dogovorov in predstavljati podlago zanje, ***v primeru*** vsaj ***sklopa*** okoliščin, ki kažejo na ***resne*** izpade pri tretjem ponudniku storitev IKT***, pa bi bilo treba sprejeti popravljalne in sanacijske ukrepe, ki bi lahko vključevali delno ali popolno odpoved*** pogodb.

(49) Za obravnavo sistemskega učinka tveganja koncentracije tretjih oseb na področju IKT bi bilo treba spodbujati uravnoteženo rešitev s prilagodljivim in postopnim pristopom, saj lahko neprilagodljive zgornje meje ali stroge omejitve ovirajo poslovno ravnanje in pogodbeno svobodo. Finančni subjekti bi morali temeljito oceniti pogodbene dogovore in določiti verjetnost za pojav takega tveganja, tudi s poglobljenimi analizami dogovorov o zunanjem podizvajanju ▌. V tej fazi in zaradi doseganja poštenega ravnovesja med nujnostjo ohranjanja pogodbene svobode in nujnostjo zagotavljanja finančne stabilnosti se ne zdi ustrezno določiti strogih zgornjih mej in omejitev v zvezi z izpostavljenostjo tretjim osebam na področju IKT. ***Skupni nadzorni organ, ki izvaja nadzor*** za vsakega ključnega tretjega ponudnika storitev IKT, ***in Evropski nadzorni organ, pooblaščen za izvajanje vsakodnevnega nadzora*** (v nadaljnjem besedilu: glavni nadzornik), bi moral pri izvajanju nadzornih nalog posebno pozornost nameniti popolnemu razumevanju razsežnosti soodvisnosti in odkrivanju posebnih primerov, v katerih bo visoka stopnja koncentracije ključnih tretjih ponudnikov storitev IKT v Uniji verjetno obremenila stabilnost in celovitost finančnega sistema Unije, in bi moral v primeru opredelitve takega tveganja zagotoviti dialog s ključnimi tretjimi ponudniki storitev IKT[16].

(50) Med izvajanjem pogodb s tretjimi ponudniki storitev IKT bi bilo treba usklajevati ključne pogodbene elemente, da bi se lahko redno ocenjevala in spremljala sposobnost tretjega ponudnika storitev IKT, da finančnemu subjektu brez škodljivih učinkov na njegovo odpornost varno zagotovi storitve. Ti elementi zajemajo le minimalne pogodbene vidike, za katere finančni subjekt meni, da so ključni za celovito spremljanje z vidika zagotavljanja njegove digitalne odpornosti, ki je odvisna od stabilnosti in varnosti storitve IKT.

(51) Pogodbeni dogovori bi morali zlasti vsebovati specifikacijo podrobnih opisov funkcij in storitev, lokacij, na katerih se zagotavljajo take funkcije in obdelujejo podatki, ter navedbo celovitih opisov ravni storitev, ki jih spremljajo kvantitativni in kvalitativni

[16] Poleg tega bi morali finančni subjekti imeti možnost vložitve uradne ali neuradne pritožbe pri Evropski komisiji ali nacionalnih organih konkurenčnega prava, če se pojavi tveganje zlorabe s strani tretjega ponudnika storitev IKT, ki se šteje za prevladujočega.

cilji uspešnosti v okviru dogovorjenih ravni storitev, da se finančnemu subjektu omogoči učinkovito spremljanje. Enako bi bilo treba tudi določbe o dostopnosti, razpoložljivosti, celovitosti, varnosti in zaščiti osebnih podatkov ter jamstva za dostop, okrevanje in povračila v primeru plačilne nesposobnosti, reševanja ali prenehanja poslovanja tretjega ponudnika storitev IKT ***ali prekinitev pogodbenih dogovorov*** šteti za ključne elemente za sposobnost finančnega subjekta, da zagotovi spremljanje tveganj tretjih oseb.

(52) Da bi finančni subjekti ohranili popoln nadzor nad vsemi spremembami, ki bi lahko ogrozile njihovo varnost na področju IKT, je treba določiti odpovedne roke in obveznosti poročanja tretjega ponudnika storitev IKT v primeru sprememb, ki bi lahko pomembno vplivale na zmožnost tretjega ponudnika storitev IKT, da učinkovito izvaja kritične ali pomembne funkcije, vključno z zagotavljanjem pomoči v primeru incidenta, povezanega z IKT, ***ki je pomemben za zagotavljanje storitev ponudnika storitev IKT finančnemu subjektu na dogovorjeni ravni,*** brez dodatnih stroškov ali po ceni, ki je bila predhodno določena. ***V to uredbo niso zajete pomožne storitve IKT, od katerih finančni subjekti niso operativno odvisni.***

Poleg tega bi morala opredelitev „kritične ali pomembne funkcije“ iz te uredbe zajemati opredelitev „kritičnih funkcij“ iz točke (35) člena 2(1) Direktive 2014/59/EU Evropskega parlamenta in Sveta z dne 15. maja 2014[17]***. V skladu s tem bi morale biti funkcije, ki so kritične funkcije v skladu z Direktivo (EU) 2014/59/EU, kritične ali pomembne funkcije v smislu te uredbe.***

(53) ***V primeru pogodbenih dogovorov o izvajanju kritičnih ali pomembnih funkcij so*** pravice do dostopa, inšpekcijskega pregleda in revizije s strani finančnega subjekta ali imenovane tretje osebe ključni instrumenti pri stalnem spremljanju uspešnosti tretjega ponudnika storitev IKT, ki ga izvaja finančni subjekt, skupaj s polnim sodelovanjem slednjega med inšpekcijskimi pregledi. Tudi ***skupni nadzorni organ in vodilni nadzornik*** finančnega subjekta bi morala imeti na podlagi obvestila pravico do inšpekcijskega pregleda in revizije tretjega ponudnika storitev IKT, ob upoštevanju zaupnosti ***in previdnega ravnanja, da ne bi motila storitev, ki se zagotavljajo drugim strankam tretjega ponudnika storitev IKT***. ***Finančni subjekt in tretji ponudnik storitev IKT bi morala imeti možnost, da se dogovorita, da se pravice do dostopa, inšpekcijskega pregleda in revizije lahko prenesejo na neodvisno tretjo osebo.***

(54) Pogodbeni dogovori bi morali vključevati jasne pravice do odpovedi in z njimi povezane minimalne odpovedne roke ter namenske izhodne strategije, zlasti obvezna prehodna obdobja, v katerih bi morali tretji ponudniki storitev IKT še naprej zagotavljati ustrezne funkcije, da bi se zmanjšalo tveganje motenj na ravni finančnega subjekta ali slednjemu omogočilo, da učinkovito preide na druge tretje ponudnike storitev IKT ali da uporablja ***notranje*** rešitve v skladu z zapletenostjo zagotavljane storitve. ***Poleg tega bi morale kreditne institucije zagotoviti, da so zadevne pogodbe IKT v primeru reševanja kreditne institucije trdne in v celoti izvršljive. Kreditne institucije bi morale v skladu s***

[17] ***Direktiva 2014/59/EU Evropskega parlamenta in Sveta z dne 15. maja 2014 o vzpostavitvi okvira za sanacijo ter reševanje kreditnih institucij in investicijskih podjetij ter o spremembi Šeste direktive Sveta 82/891/EGS ter direktiv 2001/24/ES, 2002/47/ES, 2004/25/ES, 2005/56/ES, 2007/36/ES, 2011/35/EU, 2012/30/EU in 2013/36/EU in uredb (EU) št. 1093/2010 ter (EU) št. 648/2012 Evropskega parlamenta in Sveta (UL L 173, 12.6.2014, str. 190).***

pričakovanji organov za reševanje zagotoviti, da so zadevne pogodbe za storitve IKT odporne na reševanje. Dokler se kritične ali pomembne funkcije IKT še naprej izvajajo, bi morali ti finančni subjekti zagotoviti, da pogodbe med drugim vsebujejo klavzule o neprekinitvi, o neprekinitvi mirovanja in o nespreminjanju zaradi prestrukturiranja ali reševanja.

(55) Poleg tega lahko prostovoljna uporaba standardnih pogodbenih klavzul, ki jih je Komisija razvila za storitve računalništva v oblaku, finančnim subjektom in njihovim tretjim ponudnikom storitev IKT daje dodatno zagotovilo z zvišanjem stopnje pravne varnosti pri uporabi storitev računalništva v oblaku s strani finančnega sektorja, in sicer v popolni skladnosti z zahtevami in pričakovanji iz predpisov o finančnih storitvah. Ta prizadevanja temeljijo na ukrepih, predvidenih že v akcijskem načrtu za finančno tehnologijo iz leta 2018, v katerem je Komisija objavila svojo namero, da spodbudi in olajša oblikovanje standardnih pogodbenih klavzul, na podlagi katerih finančni subjekti oddajo storitve računalništva v oblaku v zunanje izvajanje, pri čemer se opira na prizadevanja zainteresiranih strani glede medsektorskih storitev računalništva v oblaku, ki jih je Komisija omogočila s pomočjo finančnega sektorja.

(55a) Evropski nadzorni organi bi morali biti pooblaščeni za pripravo osnutkov izvedbenih tehničnih in regulativnih standardov, ki določajo pričakovanja glede politik za upravljanje tveganj tretjih oseb na področju IKT in glede pogodbenih zahtev. Do začetka veljavnosti teh standardov bi morali finančni subjekti upoštevati ustrezne smernice in druge ukrepe, ki jih izdajo evropski nadzorni organi in pristojni organi.

(56) Za ključne tretje ponudnike storitev IKT bi moral veljati nazorni okvir Unije, da bi se spodbudili konvergenca in učinkovitost v zvezi z nadzornimi pristopi k tveganju tretjih oseb na področju IKT za finančni sektor, okrepila digitalna operativna odpornost finančnih subjektov, ki se pri izvajanju operativnih funkcij zanašajo na ključne tretje ponudnike storitev IKT, in da bi se tako prispevalo k ohranjanju stabilnosti finančnega sistema Unije in celovitosti enotnega trga finančnih storitev.

(57) Ker je posebna obravnava potrebna le za ključne tretje ponudnike storitev, bi bilo treba vzpostaviti mehanizem imenovanja za uporabo nadzornega okvira Unije, da bi se upoštevali razsežnost in narava odvisnosti finančnega sektorja od takih tretjih ponudnikov storitev IKT, kar pomeni sklop kvantitativnih in kvalitativnih meril, ki bi določala parametre kritičnosti kot podlago za vključitev v ***okvir nadzora***. Ključni tretji ponudniki storitev IKT, ki niso samodejno imenovani na podlagi uporabe zgoraj navedenih meril, bi morali imeti možnost, da se prostovoljno vključijo v nadzorni okvir, hkrati pa bi bilo treba izvzeti tiste tretje ponudnike storitev IKT, za katere že veljajo okviri mehanizmov nadzora, ***s katerim se podpirajo naloge*** na ravni Eurosistema iz člena 127(2) Pogodbe o delovanju Evropske unije. ***Podobno se za podjetja, ki so del finančne skupine in zagotavljajo storitve IKT izključno finančnim subjektom znotraj iste finančne skupine, ne bi smel uporabljati mehanizem za opredelitev kot kritična.***

(58) Zahteva po pravni vključitvi tretjih ponudnikov storitev IKT, ki so bili imenovani za ključne, v Unijo ne pomeni lokalizacije podatkov, saj ta uredba ne vključuje nobenih dodatnih zahtev glede potrebe po shranjevanju ali obdelavi podatkov v Uniji. ***Namen zahteve, v skladu s katero mora imeti podjetje, denimo hčerinsko podjetje, ustanovljeno v Uniji v skladu z zakonodajo države članice, je zagotoviti kontaktno točko med tretjim ponudnikom storitev IKT na eni strani ter glavnim nadzornikom in skupnim nadzornim organom na drugi strani ter zagotoviti, da lahko ta organa opravljata svoje naloge ter izvajata svoja nadzorna in izvršilna pooblastila kot je***

predvideno v tej uredbi. Pogodbenih storitev tretjega ponudnika storitev IKT njegovemu subjektu v Uniji ni treba izvajati.

(58a) Zaradi znatnega vpliva, ki bi ga lahko imela določitev kot ključnega na tretje ponudnike storitev IKT, bi bilo treba pravice do predhodnega zaslišanja določiti kot obveznost evropskih nadzornih organov in skupnega nadzornega organa, da ustrezno upoštevajo vse dodatne informacije, ki jih zagotovijo tretji ponudniki storitev IKT med postopkom imenovanja.

(59) Ta okvir ne bi smel posegati v pristojnost držav članic za izvajanje lastnih nadzornih nalog v zvezi s tretjimi ponudniki storitev IKT, ki v skladu s to uredbo niso ključni, vendar bi se šteli za pomembne na nacionalni ravni.

(60) Da bi Skupni odbor evropskih nadzornih organov izkoristil sedanjo večplastno institucionalno arhitekturo na področju finančnih storitev, bi moral še naprej zagotavljati splošno medsektorsko usklajevanje v zvezi z vsemi zadevami, povezanimi s tveganji na področju IKT, v skladu s svojimi nalogami na področju kibernetske varnosti, ***v okviru novega skupnega nadzornega organa, ki podaja*** posamezne odločitve, naslovljene na ključne tretje ponudnike storitev IKT, in skupna priporočila, zlasti glede primerjalne analize programov nadzora nad ključnimi tretjimi ponudniki storitev IKT, ter opredeljeval dobre prakse za obravnavo tveganj koncentracije na področju IKT.

(61) Za zagotovitev, da so tretji ponudniki storitev IKT, ki imajo ključno vlogo pri delovanju finančnega sektorja, sorazmerno nadzorovani na ravni Unije, ***bi bilo treba ustanoviti skupni nadzorni organ, ki bi izvajal neposredni nadzor nad ključnimi tretjimi ponudniki storitev IKT***. ***Poleg tega*** bi bilo treba enega od evropskih nadzornih organov imenovati za glavnega nadzornika za vsakega ključnega tretjega ponudnika storitev IKT***, ki opravlja in usklajuje vsakodnevni nadzor in raziskovalno delo, deluje kot enotna kontaktna točka in zagotavlja kontinuiteto***. ***Skupni nadzorni organ in vodilni nadzornik bi morala delovati nemoteno, da bi bil omogočen učinkovit dnevni nadzor ter celosten pristop k odločanju in priporočilom.***

(62) Glavni nadzorniki bi morali imeti potrebna pooblastila za izvajanje preiskav, inšpekcijske preglede ključnih tretjih ponudnikov storitev IKT na kraju samem, dostop do vseh ustreznih prostorov in lokacij ter pridobitev popolnih in posodobljenih informacij, ki bi jim omogočala pridobitev pravega vpogleda v vrsto, razsežnost in učinek tveganja tretjih oseb na področju IKT za finančne subjekte in, nazadnje, za finančni sistem Unije.

(62a) Podelitev glavne nadzorne pristojnosti ***skupnemu nadzornemu organu z neposrednim nadzorom*** je pogoj za razumevanje in obravnavanje sistemske razsežnosti tveganj na področju IKT v finančnem sektorju. Prisotnost ključnih tretjih ponudnikov storitev IKT v Uniji in morebitna povezana vprašanja glede tveganja koncentracije na področju IKT zahtevajo kolektivni pristop na ravni Unije. Ločeno izvajanje številnih revizij in pravic do dostopa s strani več pristojnih organov, pri katerem bi bilo usklajevanje omejeno ali pa ga sploh ne bi bilo, ne bi zagotovilo popolnega pregleda nad tveganjem tretjih oseb na področju IKT, hkrati pa bi ustvarilo nepotreben presežek, breme in zapletenost na ravni ključnih tretjih ponudnikov storitev IKT, ki bi se soočali s tako številnimi zahtevami.

(63) Poleg tega bi ***moral*** imeti ***skupni nadzorni organ*** možnost, da ***izda*** priporočila v zvezi s tveganji na področju IKT in ustreznimi popravnimi ukrepi, vključno z nasprotovanjem nekaterim pogodbenim dogovorom, ki nazadnje vplivajo na stabilnost finančnega

subjekta ali finančnega sistema. Pristojni nacionalni organi bi morali v okviru svoje funkcije v zvezi z bonitetnim nadzorom finančnih subjektov ustrezno upoštevati skladnost s temi vsebinskimi priporočili ***skupnega nadzornega organa***. ***Pred dokončnim oblikovanjem priporočil bi morali imeti ključni tretji ponudniki storitev IKT možnost posredovati informacije, za katere upravičeno menijo, da bi jih bilo treba upoštevati pred oblikovanjem in izdajo priporočil.***

(63a) Da se prepreči podvajanje in navzkrižja s tehničnimi in organizacijskimi ukrepi, ki se uporabljajo za ključne tretje ponudnike storitev IKT, bi morali vodilni nadzorniki in skupni nadzorni organi pri izvajanju svojih pooblastil v skladu z okvirom nadzora iz te uredbe upoštevati okvir, vzpostavljen z Direktivo (EU) 2016/1148. Pred izvajanjem teh pooblastil bi se morala skupni nadzorni organ in glavni nadzornik posvetovati z ustreznimi pristojnimi organi iz Direktive (EU) 2016/1148.

(64) Okvir nadzora ne zamenjuje ali kakor koli nadomešča upravljanja tveganj, ki ga finančni subjekti izvajajo v zvezi z uporabo tretjih ponudnikov storitev IKT, vključno z obveznostjo stalnega spremljanja pogodbenih dogovorov, sklenjenih s ključnimi tretjimi ponudniki storitev IKT, in ne vpliva na polno odgovornost finančnih subjektov, da upoštevajo in izpolnijo vse zahteve iz te uredbe in ustrezne zakonodaje o finančnih storitvah. Da bi se izognili podvajanju in prekrivanju, pristojni organi ne bi smeli ločeno sprejemati ukrepov, namenjenih spremljanju tveganj ključnih tretjih ponudnikov storitev IKT. Vsak tak ukrep bi bilo treba predhodno uskladiti in se o njem dogovoriti na podlagi nadzornega okvira.

(65) Evropske nadzorne organe bi bilo treba spodbujati, da sklenejo dogovore o sodelovanju z ustreznimi nadzornimi in regulativnimi pristojnimi organi tretjih držav, da bi se olajšal razvoj dobrih praks za obravnavanje tveganj tretjih oseb na področju IKT in da bi se tako na mednarodni ravni spodbujala konvergenca dobrih praks, ki naj se uporabljajo pri reviziji upravljanja digitalnih tveganj tretjih ponudnikov storitev IKT.

(66) Da bi glavni nadzorniki ***pri izvajanju splošnih preiskav in inšpekcijskih pregledov na kraju samem*** izkoristili tehnično strokovno znanje strokovnjakov pristojnih organov za upravljanje operativnih tveganj in tveganj na področju IKT, bi morali črpati iz izkušenj nacionalnih nadzornikov ter za vsakega posameznega ključnega tretjega ponudnika storitev IKT ustanoviti posebne pregledniške ekipe, ki bi združevale multidisciplinarne skupine za podporo pri pripravi in dejanskem izvajanju nadzornih dejavnosti, vključno z inšpekcijskimi pregledi ključnih tretjih ponudnikov storitev IKT na kraju samem, ter pri njihovem nadaljnjem spremljanju.

(67) Pristojni organi bi morali imeti vsa potrebna pooblastila za nadzor, preiskovanje in izrekanje sankcij, da se zagotovi uporaba te uredbe. Upravne kazni bi načeloma morale biti objavljene. Ker so lahko finančni subjekti in tretji ponudniki storitev IKT ustanovljeni v različnih državah članicah in pod nadzorom različnih sektorskih pristojnih organov, bi bilo treba zagotoviti tesno sodelovanje med ustreznimi pristojnimi organi, vključno z Evropsko centralno banko (ECB) v zvezi s posebnimi nalogami, ki so nanjo prenesene z Uredbo Sveta (EU) št. 1024/2013[18], in posvetovanje z evropskimi nadzornimi organi, in sicer z izmenjavo informacij ter zagotavljanjem pomoči pri nadzornih dejavnostih. ***Čeprav enotni odbor za reševanje ni pristojni organ za namene***

[18] Uredba Sveta (EU) št. 1024/2013 z dne 15. oktobra 2013 o prenosu posebnih nalog, ki se nanašajo na politike bonitetnega nadzora kreditnih institucij, na Evropsko centralno banko (UL L 287, 29.10.2013, str. 63).

te uredbe, bi moral biti vseeno vključen v mehanizme za medsebojno izmenjavo informacij za subjekte, ki spadajo na področje uporabe Uredbe (EU) št. 806/2014 Evropskega parlamenta in Sveta[19].

(68) Za nadaljnjo kakovostno in količinsko opredelitev meril v zvezi z imenovanjem ključnih tretjih ponudnikov storitev IKT in za uskladitev nadomestil za nadzor bi bilo treba na Komisijo prenesti pooblastilo, da bi lahko v skladu s členom 290 Pogodbe o delovanju Evropske unije sprejemala akte v zvezi z naslednjimi vidiki: nadaljnja opredelitev sistemskega učinka, ki bi ga prenehanje delovanja tretjega ponudnika storitev IKT lahko imelo na finančne subjekte, ki jim zagotavlja storitve, število globalnih sistemsko pomembnih institucij (GSPI) ali drugih sistemsko pomembnih institucij (DSPI), ki so odvisne od zadevnega tretjega ponudnika storitev IKT, število tretjih ponudnikov storitev IKT, ki delujejo na posameznem trgu, stroški prehoda na drugega tretjega ponudnika storitev IKT, število držav članic, v katerih zadevni tretji ponudnik storitev IKT zagotavlja storitve in v katerih poslujejo finančni subjekti, ki uporabljajo zadevnega tretjega ponudnika storitev IKT, ter znesek nadomestil za nadzor in način njihovega plačila.

Zlasti pomembno je, da se Komisija pri svojem pripravljalnem delu ustrezno posvetuje, tudi s strokovnjaki, in da se posvetovanje izvede v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje[20]. Za zagotovitev enakopravnega sodelovanja pri pripravi delegiranih aktov Evropski parlament in Svet prejmeta vse dokumente sočasno s strokovnjaki iz držav članic, njuni strokovnjaki pa se sistematično lahko udeležujejo sestankov strokovnih skupin Komisije, ki zadevajo pripravo delegiranih aktov.

(69) Ker ta uredba, skupaj z Direktivo (EU) 20xx/xx Evropskega parlamenta in Sveta[21], vključuje konsolidacijo določb o upravljanju tveganj na področju IKT, ki jih vsebujejo številne uredbe in direktive pravnega reda Unije na področju finančnih storitev, vključno z uredbami (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014 in (EU) št. 909/2014, bi bilo treba za zagotovitev popolne skladnosti vse navedene uredbe spremeniti in tako pojasniti, da so ustrezne določbe, povezane s tveganji na področju IKT, opredeljene v tej uredbi.

V konsolidacijskem procesu bi bilo treba ustrezne smernice za uporabo teh uredb in direktiv, ki jih izdajo ali ki jih ravno pripravljajo evropski nadzorni organi, pregledati in revidirati, zato da bi bila v zakonodaji Unije pravna podlaga za zahteve glede tveganj na področju IKT, povezanih s subjekti s področja uporabe te uredbe, oprta izključno na to uredbo, njene izvedbene akte ter na sklepe in priporočila, sprejeta v skladu z njo.

(69a) Dosledno harmonizacijo zahtev iz te uredbe bi bilo treba zagotoviti s tehničnimi standardi. Ker imajo evropski nadzorni organi visokospecializirano strokovno znanje, bi morali biti pooblaščeni za pripravo osnutkov regulativnih tehničnih standardov, ki ne bodo vključevali odločitev politike, in bi jih morali predložiti Komisiji. Regulativne tehnične standarde je treba razviti za področja upravljanja tveganj na področju IKT,

---

19 ***Uredba (EU) št. 806/2014 Evropskega parlamenta in Sveta z dne 15. julija 2014 o določitvi enotnih pravil in enotnega postopka za reševanje kreditnih institucij in določenih investicijskih podjetij v okviru enotnega mehanizma za reševanje in enotnega sklada za reševanje ter o spremembi Uredbe (EU) št. 1093/2010 (UL L 225, 30.7.2014, str. 1)***

20 UL L 123, 12.5.2016, str. 1.

21 [*Vstaviti celotni sklic.*]

poročanja, testiranja in ključnih zahtev za dobro spremljanje tveganj tretjih oseb na področju IKT. ***Pri oblikovanju osnutkov regulativnih tehničnih standardov bi morali evropski nadzorni organi upoštevati svoja pooblastila v zvezi z vidiki sorazmernosti in se posvetovati s posvetovalnimi odbori za sorazmernost, zlasti glede uporabe te uredbe za mala in srednja podjetja ter podjetja s srednje veliko tržno kapitalizacijo.***

(70) Zlasti pomembno je, da se Komisija pri svojem pripravljalnem delu ustrezno posvetuje, tudi na ravni strokovnjakov. Komisija in evropski nadzorni organi bi morali zagotoviti, da bi lahko te standarde in zahteve vsi finančni subjekti uporabljali tako, da bi ustrezalo naravi, obsegu in zapletenosti teh subjektov in tudi njihovih dejavnosti.

(71) Za lažjo primerljivost poročil o večjih incidentih, povezanih z IKT, in da se zagotovi preglednost pogodbenih dogovorov o uporabi storitev IKT, ki jih zagotavljajo tretji ponudniki storitev IKT, bi morali biti evropski nadzorni organi pooblaščeni za pripravo osnutkov izvedbenih tehničnih standardov, s katerimi bi določili standardizirane predloge, obrazce in postopke, s katerimi bi finančni subjekti poročali o večjem incidentu, povezanem z IKT, ter standardizirane predloge za register informacij. Evropski nadzorni organi bi morali pri oblikovanju teh standardov upoštevati ***naravo,*** velikost, kompleksnost ***in poslovni profil*** finančnih subjektov ter naravo in stopnjo tveganja njihovih dejavnosti. Na Komisijo bi bilo treba prenesti pooblastilo za sprejetje navedenih izvedbenih tehničnih standardov z izvedbenimi akti v skladu s členom 291 PDEU ter členom 15 Uredbe (EU) št. 1093/2010, (EU) št. 1094/2010 oziroma (EU) št. 1095/2010. Ker so bile nadaljnje zahteve že določene z delegiranimi in izvedbenimi akti, ki temeljijo na tehničnih regulativnih in izvedbenih tehničnih standardih v Uredbi (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014 oziroma (EU) št. 909/2014, je ustrezno pooblastiti evropske nadzorne organe, da bodisi posamično bodisi skupaj prek Skupnega odbora Komisiji predložijo regulativne in izvedbene tehnične standarde za sprejetje delegiranih in izvedbenih aktov, s katerimi se prenašajo in posodabljajo obstoječa pravila o upravljanju tveganj na področju IKT.

(72) To bo vključevalo naknadne spremembe že obstoječih delegiranih in izvedbenih aktov, sprejetih na različnih področjih zakonodaje o finančnih storitvah. Področje uporabe členov o operativnem tveganju, na podlagi katerih so bili v skladu s pooblastili v navedenih aktih sprejeti delegirani in izvedbeni akti, je treba spremeniti, da se v to uredbo prenesejo vse določbe o digitalni operativni odpornosti, ki so trenutno del navedenih uredb.

(73) Ker države članice zaradi nujno potrebne harmonizacije številnih različnih pravil, ki trenutno obstajajo bodisi v nekaterih aktih Unije bodisi v pravnih sistemih različnih držav članic, ne morejo zadovoljivo doseči ciljev te uredbe, namreč visoke stopnje digitalne operativne odpornosti vseh finančnih subjektov, temveč se ti cilji zaradi obsega in učinkov te uredbe lažje dosežejo na ravni Unije, lahko Unija sprejme ukrepe v skladu z načelom subsidiarnosti, kot je določeno v členu 5 Pogodbe o Evropski uniji. V skladu z načelom sorazmernosti, kot je določeno v navedenem členu, ta uredba ne presega okvirov, ki so potrebni za dosego navedenega cilja –

SPREJELA NASLEDNJO UREDBO:

POGLAVJE I

SPLOŠNE DOLOČBE

Člen 1

Predmet urejanja

1. Ta uredba določa naslednje enotne zahteve glede varnosti omrežja in informacijskih sistemov, pri čemer podpira poslovne procese finančnih subjektov, potrebne za doseganje visoke skupne stopnje digitalne operativne odpornosti:

(a) zahteve, ki veljajo za finančne subjekte glede:

– upravljanja tveganj na področju informacijske in komunikacijske tehnologije (IKT);

– poročanja pristojnim organom o večjih incidentih, povezanih z IKT;

– ***poročanja finančnih subjektov iz člena 2(1), točk (a) do (c) pristojnim organom o večjih operativnih ali varnostnih incidentih, povezanih s plačili;***

– testiranja digitalne operativne odpornosti;

– izmenjave informacij in obveščevalnih podatkov v zvezi s kibernetskimi grožnjami in ranljivostmi;

– ukrepov ***finančnih subjektov*** za dobro upravljanje tveganj tretjih oseb na področju IKT ▌;

(b) zahteve v zvezi s pogodbenimi dogovori, sklenjenimi med tretjimi ponudniki storitev IKT in finančnimi subjekti;

(c) okvir nadzora za ključne tretje ponudnike storitev IKT, ki zagotavljajo storitve finančnim subjektom;

(d) pravila o sodelovanju med pristojnimi organi in pravila o nadzoru in izvrševanju s strani pristojnih organov v zvezi z vsemi zadevami, zajetimi v tej uredbi.

2. V zvezi s finančnimi subjekti, opredeljenimi kot izvajalci bistvenih storitev v skladu z nacionalnimi pravili, s katerimi je prenesen člen 5 Direktive (EU) 2016/1148, se ta uredba za namene člena 1(7) navedene direktive šteje za sektorski pravni akt Unije.

2a. Ta uredba ne posega v pristojnosti držav članic glede zagotavljanja javne varnosti, obrambe in državne varnosti.

Člen 2

Osebno področje uporabe

1. Ta uredba se uporablja za naslednje subjekte:

(a) kreditne institucije,

(b) plačilne institucije,

(c) institucije za izdajo elektronskega denarja,

(d) investicijska podjetja,

(e) ponudnike storitev v zvezi s kriptoimetji, izdajatelje ***in ponudnike*** kriptoimetij,

izdajatelje ***in ponudnike*** žetonov, vezanih na sredstva, in izdajatelje pomembnih žetonov, vezanih na sredstva,

(f) centralne depotne družbe ***in upravljavce sistemov poravnave vrednostnih papirjev***,

(g) centralne nasprotne stranke,

(h) mesta trgovanja,

(i) repozitorije sklenjenih poslov,

(j) upravitelje alternativnih investicijskih skladov,

(k) družbe za upravljanje,

(l) izvajalce storitev sporočanja podatkov,

(m) zavarovalnice in pozavarovalnice,

(n) zavarovalne posrednike, pozavarovalne posrednike in posrednike dopolnilnih zavarovanj***, ki niso mikro, mala ali srednja podjetja, razen če so ta mikro, mala ali srednja podjetja odvisna izključno od organiziranih avtomatiziranih prodajnih sistemov***,

(o) institucije za ***zagotavljanje poklicnega pokojninskega zavarovanja, ki ne upravljajo pokojninskih načrtov z manj kot 15 člani***,

(p) bonitetne agencije,

(q) zakonite revizorje in revizijska podjetja***, ki niso mikro, mala ali srednja podjetja, razen če ta mikro, mala ali srednja podjetja opravljajo revizijske storitve za subjekte iz tega člena, razen za mikro, mala in srednja podjetja, ki so nepridobitni revizijski subjekti v skladu s členom 2(3) Uredbe (EU) št. 537/2014, razen če pristojni organ odloči, da izjema ni veljavna***,

(r) upravljavce ključnih referenčnih vrednosti,

(s) ponudnike storitev množičnega financiranja,

(t) repozitorije listinjenja,

(u) tretje ponudnike storitev IKT.

1a. Ta uredba, razen oddelka II poglavja V, se uporablja tudi za ponudnike storitev IKT znotraj skupine.

2. Za namene te uredbe se subjekti iz odstavkov (a) do (t) skupaj imenujejo „finančni subjekti“.

2a. V tej uredbi, z izjemo oddelka II poglavja V, se tretji ponudniki storitev IKT in ponudniki storitev IKT znotraj skupine skupaj imenujejo „tretji ponudniki storitev IKT“.

Člen 3

Opredelitve pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(1) „digitalna operativna odpornost“ pomeni zmožnost finančnega subjekta, da vzpostavi, zagotavlja in pregleduje svojo operativno integriteto ▌ tako, da neposredno ali posredno

z uporabo storitev tretjih ponudnikov storitev IKT zagotovi ▌neprekinjeno zagotavljanje in kakovost finančnih storitev ***kljub operativnim motnjam, ki negativno vplivajo na zmogljivosti finančnega subjekta na področju IKT***;

(2) „omrežje in informacijski sistem“ pomeni omrežje in informacijski sistem, kot sta opredeljena v točki 1 člena 4 Direktive (EU) 2016/1148;

(3) „varnost omrežij in informacijskih sistemov“ pomeni varnost omrežij in informacijskih sistemov, kot je opredeljena v točki 2 člena 4 Direktive (EU) 2016/1148;

(4) „tveganja na področju IKT“ pomenijo vsako razumno določljivo okoliščino v zvezi z uporabo omrežja in informacijskih sistemov, ▌ki lahko, če se uresniči, ogrozi varnost omrežja in informacijskih sistemov, orodij ali postopkov, odvisnih od ***IKT***, varnost delovanja in izvajanja postopkov ali zagotavljanja storitev ▌;

(5) „informacijsko sredstvo“ pomeni zbirko oprijemljivih ali neoprijemljivih informacij, ki jih je vredno zavarovati;

(6) „incident, povezan z IKT“ pomeni nepredviden ugotovljen dogodek ***ali vrsto povezanih incidentov***, ki ▌ogrožajo varnost omrežja in informacijskih sistemov ▌ali imajo škodljiv učinek na razpoložljivost, zaupnost, neprekinjenost***, celovitost*** ali verodostojnost finančnih storitev, ki jih zagotavlja finančni subjekt;

(6a) „operativni ali varnostni incident, povezan s plačili“ pomeni dogodek ali vrsto povezanih dogodkov, ki jih finančni subjekti iz člena 2(1), točk (a) do (c) niso predvideli in negativno vplivajo ali bi lahko negativno vplivali na celovitost, razpoložljivost, zaupnost, avtentičnost ali kontinuiteto storitev, povezanih s plačili;

(7) „večji incident, povezan z IKT“ pomeni incident, povezan z IKT, ***z velikim ali*** potencialnim velikim škodljivim učinkom na omrežje in informacijske sisteme, ki podpirajo kritične funkcije finančnega subjekta;

(7a) „večji operativni ali varnostni incident, povezan s plačili“ pomeni operativni ali varnostni incident, povezan s plačili, ki izpolnjuje merila iz člena 16;

(8) „kibernetska grožnja“ pomeni kibernetsko grožnjo, kot je opredeljena v točki 8 člena 2 Uredbe (EU) št. 2019/881 Evropskega parlamenta in Sveta[22];

(8a) „znatna kibernetska grožnja“ pomeni kibernetsko grožnjo, ki utegne zaradi svojih značilnosti povzročiti večji incident, povezan z IKT;

(9) „kibernetski napad“ pomeni zlonameren incident, povezan z IKT, s katerim poskuša akter grožnje uničiti, razkriti, spremeniti, onemogočiti ali ukrasti sredstvo, pridobiti nepooblaščen dostop do njega ali ga nedovoljeno uporabiti;

(10) „obveščevalni podatki o grožnjah“ pomenijo informacije, ki so bile združene, preoblikovane, analizirane, razložene ali obogatene, da bi zagotovile potreben okvir za odločanje, in ki prinašajo ustrezno in zadostno razumevanje za zmanjšanje učinka incidenta, povezanega z IKT, ali kibernetske grožnje, vključno s tehničnimi podrobnostmi kibernetskega napada ter podatki o odgovornih osebah za napad, njihovem načinu delovanja in motivih;

---

[22] Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L 151, 7.6.2019, str. 15).

(11) „obramba v globino“ pomeni strategijo, povezano z IKT, ki zajema ljudi, postopke in tehnologijo za vzpostavitev različnih ovir na številnih ravneh in razsežnostih subjekta;

(12) „ranljivost“ pomeni šibkost, dovzetnost ali napako sredstva, sistema, postopka ali nadzora, ki jo ***kibernetska*** grožnja lahko izkoristi;

(13) „penetracijsko testiranje na podlagi analize groženj“ pomeni okvir, ki posnema taktike, tehnike in postopke dejanskih akterjev groženj, za katere se šteje, da predstavljajo resnično kibernetsko grožnjo, in ki zagotavlja nadzorovan, prilagojen in na podlagi obveščevalnih podatkov (rdeča ekipa) oblikovan test ključnih aktivnih produkcijskih sistemov subjekta;

(14) „tveganje tretjih oseb na področju IKT“ pomeni tveganje na področju IKT, ki lahko grozi finančnemu subjektu zaradi njegove uporabe storitev IKT, ki jih zagotavljajo tretji ponudniki storitev IKT ali njihovi nadaljnji podizvajalci;

(15) „tretji ponudnik storitev IKT“ pomeni podjetje, ki zagotavlja ▌ storitve ***IKT***, vključno s finančnimi subjekti, ki zagotavljajo storitve IKT in so del podjetja, ki zagotavlja širši nabor proizvodov ali storitev, vendar brez ponudnikov komponent strojne opreme in podjetij, pooblaščenih v okviru prava Unije, ki zagotavljajo elektronske komunikacijske storitve iz točke 4 člena 2 Direktive (EU) 2018/1972 Evropskega parlamenta in Sveta[23];

(15a) „ponudnik storitev IKT znotraj skupine“ pomeni podjetje, ki je del finančne skupine in zagotavlja storitve IKT izključno finančnim subjektom v isti skupini ali finančnim subjektom, ki spadajo v isto institucionalno jamstveno shemo, vključno z nadrejenimi in podrejenimi podjetji, podružnicami ali subjekti, ki so pod skupnim lastništvom ali nadzorom;

(16) „storitve IKT“ pomenijo digitalne in podatkovne storitve, ki se prek sistemov IKT ***neprekinjeno*** zagotavljajo enemu ali več notranjim ali zunanjim uporabnikom***, razen telekomunikacijskih pogodb***;

(17) „kritična ali pomembna funkcija“ pomeni ***dejavnost ali storitev, ki je odločilnega pomena za delovanje finančnega subjekta in pri kateri bi motnja bistveno ogrozila trdnost ali neprekinjenost njegovih storitev in dejavnosti ali*** katere prekinjeno, pomanjkljivo ali neuspešno izvajanje bi bistveno oviralo neprekinjeno skladnost finančnega subjekta s pogoji in obveznostmi njegovega dovoljenja ali drugimi obveznostmi v skladu z veljavno zakonodajo o finančnih storitvah***, vključno s „kritičnimi funkcijami“, kot so opredeljene v členu 2, odstavku 1, točki 35 Direktive 2014/59/EU***;

(18) „ključni tretji ponudnik storitev IKT“ pomeni tretjega ponudnika storitev IKT, imenovanega v skladu s členom ***28***, za katerega velja okvir nadzora iz členov ***29*** do 37;

(19) „tretji ponudnik storitev IKT s sedežem v tretji državi“ pomeni tretjega ponudnika storitev IKT, ki je pravna oseba s sedežem v tretji državi ▌ in ki je sklenil pogodbeni dogovor s finančnim subjektom za zagotavljanje storitev IKT;

(20) „podizvajalec storitev IKT s sedežem v tretji državi“ pomeni podizvajalca storitev IKT, ki je pravna oseba s sedežem v tretji državi ▌ in ki je sklenil pogodbeni dogovor bodisi s tretjim ponudnikom storitev IKT ali tretjim ponudnikom storitev IKT s sedežem v

[23] Direktiva (EU) 2018/1972 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o Evropskem zakoniku o elektronskih komunikacijah (prenovitev) (UL L 321, 17.12.2018, str. 36).

tretji državi;

(21) „tveganje koncentracije na področju IKT“ pomeni izpostavljenost enemu ali več povezanim ključnim tretjim ponudnikom storitev IKT, ki ustvarja določeno stopnjo odvisnosti od teh ponudnikov, tako da lahko njihova nedosegljivost, nezmožnost opravljanja storitev ali druga vrsta izpada potencialno ogrozi ***finančno stabilnost vse Unije ali*** zmožnost finančnega subjekta ▌, da opravlja kritične ali pomembne funkcije, ali pa mu povzroči druge vrste škodljivih učinkov, vključno z velikimi izgubami;

(22) „upravljalni organ“ pomeni upravljalni organ, kot je opredeljen v točki 36 člena 4(1) Direktive 2014/65/EU, točki 7 člena 3(1) Direktive 2013/36/EU, točki (s) člena 2(1) Direktive 2009/65/ES, točki 45 člena 2(1) Uredbe (EU) št. 909/2014, točki 20 člena 3(1) Uredbe (EU) 2016/1011 Evropskega parlamenta in Sveta[24], točki (***18***) člena 3(1) Uredbe (EU) 20xx/xx Evropskega parlamenta in Sveta[25] [MiCA], ali enakovredne osebe, ki dejansko vodijo subjekt ali imajo kritične funkcije v skladu z ustrezno zakonodajo Unije ali nacionalno zakonodajo;

(23) „kreditna institucija“ pomeni kreditno institucijo, kot je opredeljena v točki 1 člena 4(1) Uredbe (EU) št. 575/2013 Evropskega parlamenta in Sveta[26];

(23a) „kreditna institucija, izvzeta z Direktivo 2013/36/EU“ pomeni institucijo, ki je izvzeta po členu 2(5), točkah (4) do (23) Direktive 2013/36/EU;

(24) „investicijsko podjetje“ pomeni investicijsko podjetje, kot je opredeljeno v točki 1 člena 4(1) Direktive 2014/65/EU;

(24a) „malo in nepovezano investicijsko podjetje“ pomeni investicijsko podjetje, ki izpolnjuje pogoje iz člena 12(1) Uredbe (EU) 2019/2033;

(25) „plačilna institucija“ pomeni plačilno institucijo, kot je opredeljena v točki (d) člena 1(1) Direktive (EU) št. 2015/2366;

(25a) „plačilna institucija, izvzeta z Direktivo (EU) 2015/2366“ pomeni plačilno institucijo, ki je izvzeta po členu 32(1) Direktive (EU) št. 2015/2366;

(26) „institucija za izdajo elektronskega denarja“ pomeni institucijo za izdajo elektronskega denarja, kot je opredeljena v točki 1 člena 2 Direktive 2009/110/ES Evropskega parlamenta in Sveta[27];

(26a) „institucija za izdajo elektronskega denarja, izvzeta z Direktivo 2009/110/ES“ pomeni institucijo za izdajo elektronskega denarja, ki je izvzeta po členu 9 Direktive 2009/110/ES;

(27) „centralna nasprotna stranka“ pomeni centralno nasprotno stranko, kot je opredeljena v

---

24 Uredba (EU) 2016/1011 Evropskega parlamenta in Sveta z dne 8. junija 2016 o indeksih, ki se uporabljajo kot referenčne vrednosti v finančnih instrumentih in finančnih pogodbah ali za merjenje uspešnosti investicijskih skladov, in spremembi direktiv 2008/48/ES in 2014/17/EU ter Uredbe (EU) št. 596/2014 (UL L 171, 29.6.2016, str. 1).

25 [*Vstaviti polni naslov in podatke o UL.*]

26 Uredba (EU) št. 575/2013 Evropskega parlamenta in Sveta z dne 26. junija 2013 o bonitetnih zahtevah za kreditne institucije in investicijska podjetja ter o spremembi Uredbe (EU) št. 648/2012 (UL L 176, 27.6.2013, str. 1).

27 Direktiva 2009/110/ES Evropskega parlamenta in Sveta z dne 16. septembra 2009 o začetku opravljanja in opravljanju dejavnosti ter nadzoru skrbnega in varnega poslovanja institucij za izdajo elektronskega denarja ter o spremembah direktiv 2005/60/ES in 2006/48/ES in razveljavitvi Direktive 2000/46/ES (UL L 267, 10.10.2009, str. 7).

točki 1 člena 2 Uredbe (EU) št. 648/2012;

(28) „repozitorij sklenjenih poslov“ pomeni repozitorij sklenjenih poslov, kot je opredeljen v točki 2 člena 2 Uredbe (EU) št. 648/2012;

(29) „centralna depotna družba“ pomeni centralno depotno družbo, kot je opredeljena v točki 1 člena 2(1) Uredbe (EU) št. 909/2014;

(30) „mesto trgovanja“ pomeni mesto trgovanja, kot je opredeljeno v točki 24 člena 4(1) Direktive 2014/65/EU;

(31) „upravitelj alternativnih investicijskih skladov“ pomeni upravitelja alternativnih investicijskih skladov, kot je opredeljen v točki (b) člena 4(1) Direktive 2011/61/EU;

(32) „družba za upravljanje“ pomeni družbo za upravljanje, kot je opredeljena v točki (b) člena 2(1) Direktive 2009/65/ES;

(33) „izvajalec storitev sporočanja podatkov“ pomeni izvajalca storitev sporočanja podatkov, kot je opredeljen v točki 63 člena 4(1) Direktive 2014/65/EU;

(34) „zavarovalnica“ pomeni zavarovalnico, kot je opredeljena v točki 1 člena 13 Direktive 2009/138/ES;

(35) „pozavarovalnica“ pomeni pozavarovalnico, kot je opredeljena v točki 4 člena 13 Direktive 2009/138/ES;

(36) „zavarovalni posrednik“ pomeni zavarovalnega posrednika, kot je opredeljen v točki 3 člena 2***(1)*** Direktive (EU) 2016/97;

(37) „posrednik dopolnilnih zavarovanj“ pomeni posrednika dopolnilnih zavarovanj, kot je opredeljen v točki 4 člena 2***(1)*** Direktive (EU) 2016/97;

(38) „pozavarovalni posrednik“ pomeni pozavarovalnega posrednika, kot je opredeljen v točki 5 člena 2***(1)*** Direktive (EU) 2016/97;

(39) „institucija za poklicno pokojninsko zavarovanje“ pomeni institucijo za poklicno pokojninsko zavarovanje, kot je opredeljena v točki 6 člena 1 Direktive 2016/2341;

(40) „bonitetna agencija“ pomeni bonitetno agencijo, kot je opredeljena v točki (a) člena 3(1) Uredbe (ES) št. 1060/2009;

(41) „zakoniti revizor“ pomeni zakonitega revizorja, kot je opredeljen v točki 2 člena 2 Direktive 2006/43/ES;

(42) „revizijsko podjetje“ pomeni revizijsko podjetje, kot je opredeljeno v točki 3 člena 2 Direktive 2006/43/ES;

(43) „ponudnik storitev v zvezi s kriptoimetji“ pomeni ponudnika storitev v zvezi s kriptoimetji, kot je opredeljen v točki (***8***) člena 3(1) Uredbe (EU) 202x/xx [UP: vstaviti sklic na uredbo MiCA];

(44) „izdajatelj kriptoimetij“ pomeni izdajatelja kriptoimetij, kot je opredeljen v točki (***6***) člena 3(1) [UL: vstaviti sklic na uredbo MiCA];

(44a) „ponudnik“ pomeni ponudnika, kot je opredeljen v točki [(XX)] člena 3(1) [UL: vstaviti sklic na uredbo MiCA];

(44b) „ponudnik kriptoimetij“ pomeni ponudnika kriptoimetij, kot je opredeljen v točki [(XX) člena 3 (1)] [UL: vstaviti sklic na uredbo MiCA];

(45) „izdajatelj žetonov, vezanih na sredstva“ pomeni izdajatelja žetonov, vezanih na sredstva, kot je opredeljen v točki (i) člena 3(1) [UL: vstaviti sklic na uredbo MiCA];

(45a) „ponudnik žetonov, vezanih na sredstva“ pomeni ponudnika žetonov, vezanih na sredstva, kot je opredeljen v točki [(XX)] člena 3(1) [UL: vstaviti sklic na uredbo MiCA];

(46) „izdajatelj pomembnih žetonov, vezanih na sredstva“ pomeni izdajatelja pomembnih žetonov, vezanih na sredstva, kot je opredeljen v točki (***XX***) člena 3(1) [UL: vstaviti sklic na uredbo MiCA];

(47) „upravljavec ključnih referenčnih vrednosti“ pomeni upravljavca ključnih referenčnih vrednosti, kot je opredeljen v točki (***25***) člena ***3*** Uredbe ***2016/1011*** [UL: vstaviti sklic na uredbo o referenčnih vrednostih];

(48) „ponudnik storitev množičnega financiranja“ pomeni ponudnika storitev množičnega financiranja, kot je opredeljen v točki ***(e)*** člena ***2(1)*** Uredbe (EU) ***2020/1503*** [UP: vstaviti sklic na uredbo o množičnem financiranju];

(49) „repozitorij listinjenj“ pomeni repozitorij listinjenj, kot je opredeljen v točki 23 člena 2 Uredbe (EU) 2017/2402;

(50) „mikro***, malo in srednje*** podjetje“ pomeni finančni subjekt, kot je opredeljen v členu 2 Priloge k Priporočilu 2003/361/ES;

(50a) „organ za reševanje“ pomeni organ, ki ga v skladu s členom 3 Direktive 2014/59/EU določi država članica, ali enotni odbor za reševanje v skladu s členom 42 Uredbe (EU) št. 806/2014.

Člen 3a

Načelo sorazmernosti

1. Finančni subjekti izvajajo pravila iz poglavij II, III in IV v skladu z načelom sorazmernosti, pri tem pa upoštevajo svojo velikost, naravo, obseg in kompleksnost svojih storitev, dejavnosti in operacij ter svoj splošni profil tveganja.

2. V skladu z načelom sorazmernosti se členi 4 do 14 te uredbe ne uporabljajo za:

(a) mala in nepovezana investicijska podjetja ali plačilne institucije, izvzete z Direktivo (EU) 2015/2366;

(b) kreditne institucije, izvzete z Direktivo 2013/36/EU;

(c) institucije za izdajo elektronskega denarja, izvzete z Direktivo 2009/110/ES, ali

(d) male institucije za poklicno pokojninsko zavarovanje.

3. Pristojni organi na podlagi letnega poročila o pregledu okvira za upravljanje tveganj na področju IKT iz členov 5(6) in 14a(2) pregledajo in ovrednotijo, kako finančni subjekt uveljavlja sorazmernost, in ugotovijo, ali okvir finančnega subjekta za upravljanje tveganj na področju IKT zagotavlja dobro upravljanje ter digitalno operativno odpornost in kritje tveganj na področju IKT. Pri tem upoštevajo velikost finančnega subjekta ter naravo, obseg in kompleksnost njegovih storitev, dejavnosti in poslovanja pa tudi njegov splošni profil tveganja.

4. Če pristojni organ presodi, da okvir finančnega subjekta za upravljanje tveganj na področju IKT ni zadosten in sorazmeren, z njim naveže dialog, da se pomanjkljivosti odpravijo in da se zagotovi popolna skladnost s poglavjem II.

5. Evropski nadzorni organi pripravijo osnutke regulativnih tehničnih standardov, s katerimi:

(a) določijo, katere obveznosti upravljanja tveganj na področju IKT se uporabijo pri vsakem od finančnih subjektov iz odstavka 1;

(b) opredelijo vsebino in obliko letnega poročila o pregledu okvira za upravljanje tveganj na področju IKT iz odstavka 3;

(c) določijo pravila in postopke, ki jih morajo pristojni organi in finančni subjekti upoštevati v dialogu iz odstavka 4.

6. Evropski nadzorni organi osnutke regulativnih tehničnih standardov iz odstavka 5 Komisiji predložijo do [UL: vstaviti datum eno leto po datumu začetka veljavnosti].

Na Komisijo se prenese pooblastilo za sprejetje regulativnih tehničnih standardov iz prvega pododstavka v skladu s členi 10 do 14 Uredbe (EU) št. 1093/2010, (EU) št. 1094/2010 oziroma (EU) št. 1095/2010.

POGLAVJE II

UPRAVLJANJE TVEGANJ NA PODROČJU IKT

ODDELEK I

Člen 4

Upravljanje in organizacija

1. Finančni subjekti vzpostavijo ***okvir*** notranjega upravljanja in ***notranjega*** nadzora, ki ***zagotavljata*** učinkovito in skrbno upravljanje vseh tveganj na področju IKT***, da bi se dosegla visoka digitalna operativna odpornost***.

2. Upravljalni organ finančnega subjekta opredeli, odobri in nadzira izvajanje vseh dogovorov, povezanih z okvirom upravljanja tveganj na področju IKT iz člena 5(1), in je odgovoren zanj.

   Za potrebe prvega pododstavka upravljalni organ:

   (a) nosi končno odgovornost za upravljanje tveganj na področju IKT, s katerimi se sooča finančni subjekt;

   (aa) uvede postopke in politike, s katerimi zagotovi spoštovanje visokih standardov varnosti, zaupnosti in celovitosti podatkov;

   (b) določi jasne vloge in odgovornosti za vse funkcije, povezane z IKT;

   (c) določi ustrezno raven tolerance tveganja na področju IKT za finančni subjekt, kot je opredeljena v točki (b) člena 5(9);

   (d) odobri, nadzira in redno pregleduje izvajanje politike finančnega subjekta za neprekinjeno poslovanje na področju IKT in njegovega načrta okrevanja IKT po katastrofi***, ki se lahko sprejme kot ločena namenska politika in kot sestavni del subjektove širše politike neprekinjenega poslovanja in načrta okrevanja po katastrofi*** iz odstavka 1 oziroma 3 člena 10;

   (e) odobri in redno pregleduje revizijske načrte na področju IKT, revizije na področju IKT in njihove bistvene spremembe;

   (f) dodeli in občasno pregleda ustrezni proračun, da lahko finančni subjekt izpolnjuje potrebe po digitalni operativni odpornosti v zvezi z vsemi vrstami virov, vključno z ***ustreznim*** usposabljanjem o tveganjih in veščinah na področju IKT za vse ▌ zaposlene;

   (g) odobri in redno pregleduje politiko finančnega subjekta glede dogovorov o uporabi storitev IKT, ki jih zagotavljajo tretji ponudniki storitev IKT;

   (h) je ustrezno obveščen o dogovorih o uporabi storitev IKT, sklenjenih s tretjimi ponudniki storitev IKT, vseh ustreznih načrtovanih pomembnih spremembah v zvezi s tretjimi ponudniki storitev IKT in možnem učinku teh sprememb na

kritične ali pomembne funkcije, za katere veljajo ti dogovori, vključno s prejetjem povzetka analize tveganja za oceno učinka teh sprememb;

(i) je ***redno*** obveščen ***vsaj*** o ***večjih*** incidentih, povezanih z IKT, in njihovem učinku ter o odzivnih, sanacijskih in popravnih ukrepih.

3. Finančni subjekti, ki niso mikro podjetja, določijo vlogo za spremljanje dogovorov ***znotraj finančnega subjekta*** o uporabi storitev IKT, ***zlasti dogovorov, sklenjenih s tretjimi ponudniki storitev IKT,*** ali določijo člana višjega vodstva, ki bo odgovoren za nadzor s tem povezane izpostavljenosti tveganju in ustrezne dokumentacije.

4. Člani upravljalnega organa ***finančnega subjekta si dejavno prizadevajo*** za pridobitev in obnavljanje zadostnega znanja in spretnosti, da lahko razumejo in ocenijo tveganja na področju IKT***, tudi z rednim namenskim usposabljanjem, primernim za tveganja na področju IKT, ki jih je treba obvladovati***.

ODDELEK II

Člen 5

Okvir za upravljanje tveganj na področju IKT

1. Finančni subjekti imajo trden, celovit in dobro dokumentiran okvir za upravljanje tveganj na področju IKT, ki jim omogoča hitro, učinkovito in celovito obravnavo tveganj na področju IKT ter zagotavljanje visoke stopnje digitalne operativne odpornosti ▌.

2. Okvir za upravljanje tveganj na področju IKT iz odstavka 1 vključuje strategije, politike, postopke, protokole in orodja IKT, ki so potrebni za pravilno in učinkovito zaščito vseh ustreznih fizičnih komponent in infrastruktur, vključno z računalniško strojno opremo, strežniki ter vsemi ustreznimi prostori, podatkovnimi centri in občutljivimi namenskimi območji, za zagotovitev, da so vsi ti fizični elementi ustrezno zaščiteni pred tveganji, vključno s škodo in nepooblaščenim dostopom ali nedovoljeno uporabo.

3. Finančni subjekti zmanjšajo vpliv tveganja na področju IKT na najmanjšo možno mero z uporabo ustreznih strategij, politik, postopkov, protokolov in orodij, kot je določeno v okviru za upravljanje tveganj na področju IKT. Zagotavljajo popolne in posodobljene informacije o tveganjih na področju IKT ***in o svojem okviru za upravljanje tveganj na področju IKT***, kot zahtevajo pristojni organi.

4. Finančni subjekti, ki niso mikro podjetja, v sklopu okvira za upravljanje tveganj na področju IKT iz odstavka 1 izvajajo sistem upravljanja informacijske varnosti, ki temelji na priznanih mednarodnih standardih in je skladen z nadzornimi smernicami, ***če so že na voljo, vključno z nasveti iz ustreznih smernic, ki jih pripravijo evropski nadzorni organi,*** ter ga redno pregledujejo.

5. Finančni subjekti, ki niso mikro podjetja, ***določijo kontrolno funkcijo z odgovornostjo za upravljanje in nadzor tveganj na področju IKT in poskrbijo za njeno neodvisnost, da se preprečijo nasprotja interesov. Finančni subjekti*** zagotovijo ustrezno ***neodvisnost*** funkcij upravljanja na področju IKT, nadzornih funkcij in funkcij notranje revizije v skladu z modelom treh obrambnih linij ali internim modelom upravljanja in nadzorovanja tveganj.

6. Okvir za upravljanje tveganj na področju IKT iz odstavka 1 se dokumentira in pregleda najmanj enkrat letno, pa tudi ob pojavu večjih incidentov, povezanih z IKT, in ob upoštevanju nadzornih navodil ali sklepov, ki izhajajo iz ustreznih postopkov testiranja ali revizije digitalne operativne odpornosti. Okvir se nenehno izboljšuje na podlagi izkušenj, pridobljenih pri izvajanju in spremljanju.

Poročilo o pregledu okvira za upravljanje tveganj na področju IKT se vsako leto posreduje pristojnemu organu.

7. Okvir za upravljanje tveganj na področju IKT iz odstavka 1 ***pri finančnih subjektih, ki niso mikro podjetja,*** redno pregledujejo revizorji s področja IKT, ki imajo zadostno znanje, spretnosti in strokovno znanje v zvezi s tveganji na področju IKT. Pogostost in osredotočenost revizij na področju IKT morata biti sorazmerni s tveganji na področju IKT, s katerimi se sooča finančni subjekt.

8. Vzpostavi se formalni postopek spremljanja, vključno s pravili za pravočasno preverjanje in sanacijo na podlagi ključnih ugotovitev revizij na področju IKT, ob upoštevanju sklepov revizijskega pregleda. ▌

9. Okvir za upravljanje tveganj na področju IKT iz odstavka 1 vključuje strategijo za digitalno ***operativno*** odpornost, ki določa, kako se okvir izvaja. V ta namen vključuje metode za obravnavanje tveganj na področju IKT in doseganje posameznih ciljev na področju IKT, tako da:

   (a) pojasni, kako okvir za upravljanje tveganj na področju IKT podpira poslovno strategijo in cilje finančnega subjekta;

   (b) določi raven tolerance tveganja na področju IKT v skladu z nagnjenostjo finančnega subjekta k prevzemanju tveganja in analizira toleranco učinka motenj na področju IKT;

   (c) določi jasne cilje glede informacijske varnosti;

   (d) pojasni ▌ arhitekturo IKT in vse spremembe, potrebne za dosego posameznih poslovnih ciljev;

   (e) opiše različne mehanizme, vzpostavljene za odkrivanje, varovanje in preprečevanje učinkov incidentov, povezanih z IKT;

   (f) dokumentira število prijavljenih večjih incidentov, povezanih z IKT, in učinkovitost preventivnih ukrepov;

   (g) opredeli ▌ključne odvisnosti od tretjih ponudnikov storitev IKT in ***opiše izhodne strategije v zvezi s temi odvisnostmi***;

   (h) izvaja testiranje digitalne operativne odpornosti ***v skladu s poglavjem IV te uredbe***;

   (i) oriše komunikacijske strategije v primeru incidentov, povezanih z IKT***, ki jih je treba v skladu s členom 13 razkriti***.

10. Po odobritvi pristojnih organov lahko finančni subjekti naloge preverjanja skladnosti z

zahtevami glede upravljanja tveganj na področju IKT prenesejo ▌ na zunanja podjetja.

Po obvestilu pristojnim organom lahko finančni subjekti naloge preverjanja skladnosti z zahtevami glede upravljanja tveganj na področju IKT prenesejo na podjetja znotraj svoje skupine.

Kjer se izvaja prenos pooblastil iz drugega pododstavka, finančni subjekt ostane v celoti odgovoren za preverjanje skladnosti z zahtevami glede upravljanja tveganj na področju IKT.

Člen 6

Sistemi, protokoli in orodja IKT

1. Finančni subjekti ***za reševanje in obvladovanje tveganj na področju IKT*** uporabljajo in vzdržujejo posodobljene sisteme, protokole in orodja IKT, ki izpolnjujejo naslednje pogoje:

   (a) sistemi in orodja so skladni z ▌ obsežnostjo operacij, ki podpirajo izvajanje njihovih dejavnosti;

   (b) so zanesljivi;

   (c) imajo zadostno zmogljivost, da pravočasno in pravilno obdelajo podatke, potrebne za izvajanje dejavnosti in opravljanje storitev, ter po potrebi obravnavajo velike količine naročil, sporočil ali poslov, tudi v primeru uvedbe nove tehnologije;

   (d) so tehnološko odporni, da se morejo ustrezno spopasti z morebitno potrebno obdelavo dodatnih informacij, kot se zahteva v stresnih tržnih razmerah ali drugih neugodnih okoliščinah.

2. Kadar finančni subjekti uporabljajo mednarodno priznane tehnične standarde in vodilne panožne prakse na področju varnosti informacij in notranjih kontrol IKT, te standarde in prakse uporabljajo v skladu z ustreznimi nadzornimi priporočili o njihovi vključitvi.

Člen 7

Opredelitev

1. Finančni subjekti v sklopu okvira za upravljanje tveganj na področju IKT iz člena 5(1) opredelijo, razvrstijo in ustrezno dokumentirajo vse ***kritične ali pomembne*** poslovne funkcije, povezane z IKT, informacijska sredstva, ki podpirajo te funkcije, ter konfiguracije sistema IKT in medsebojne povezave z notranjimi in zunanji sistemi IKT. Finančni subjekti po potrebi oziroma vsaj enkrat letno pregledajo ***kritičnost ali pomen poslovnih funkcij, povezanih z IKT,*** ter ustreznost razvrstitve informacijskih sredstev in ustrezne dokumentacije.

2. Finančni subjekti stalno opredeljujejo vse vire tveganja na področju IKT, zlasti izpostavljenost tveganju, ki ogroža druge finančne subjekte ali pa ga ti povzročajo, ter ocenjujejo kibernetske grožnje in ranljivosti na področju IKT, pomembne za njihove ***kritične ali pomembne*** poslovne funkcije in informacijska sredstva, ki so povezani z

IKT. Finančni subjekti redno oziroma vsaj enkrat letno pregledujejo scenarije tveganj, ki vplivajo nanje.

3. Finančni subjekti, ki niso mikro podjetja, ***po potrebi*** izvedejo oceno tveganja ob vsaki večji spremembi infrastrukture omrežja in infrastrukture informacijskega sistema ter procesov ali postopkov, ki vplivajo na njihove funkcije, podporne procese ali informacijska sredstva.

4. Finančni subjekti opredelijo vse račune sistemov IKT, vključno s tistimi na oddaljenih lokacijah, omrežne vire in strojno opremo ter popišejo fizično opremo, ki se šteje za ključno. Popišejo konfiguracijo ***kritičnih ali pomembnih*** sredstev IKT ***glede na namen*** ter povezave in soodvisnosti med ***temi*** sredstvi IKT.

5. Finančni subjekti opredelijo in dokumentirajo vse ***kritične ali pomembne*** postopke, ki so odvisni od tretjih ponudnikov storitev IKT, in opredelijo medsebojne povezave s tretjimi ponudniki storitev IKT***, ki podpirajo kritične ali pomembne funkcije***.

6. Finančni subjekti za namene odstavkov 1, 4 in 5 vzdržujejo in redno posodabljajo ustrezne evidence.

7. Finančni subjekti, ki niso mikro podjetja, redno oziroma vsaj enkrat letno izvajajo posebno oceno tveganj na področju IKT za vse obstoječe sisteme IKT***, tudi sisteme, ki se še vedno uporabljajo in opravljajo svoje funkcije, a so:***

   (a) stari ali proti koncu življenjske dobe, če gre za strojno opremo,

   (b) njihov dobavitelj ne zagotavlja več podpore ali vzdrževanja ali

   (c) jih ni mogoče posodobiti oziroma bi bilo to negospodarno. Za vse obstoječe sisteme IKT se izvedejo letne ocene tveganj na področju IKT, zlasti pred povezovanjem ▌ tehnologij, aplikacij ali sistemov in po njem.

Člen 8

Varovanje in preprečevanje

1. Za namene ustrezne zaščite sistemov IKT in z namenom organiziranja odzivnih ukrepov finančni subjekti stalno spremljajo in nadzirajo delovanje sistemov in orodij IKT ter z uporabo ustreznih varnostnih orodij, politik in postopkov na področju IKT na najmanjšo možno mero zmanjšujejo učinek tovrstnih tveganj.

2. Finančni subjekti oblikujejo, pridobijo in izvajajo varnostne strategije, politike, postopke, protokole in orodja na področju IKT, katerih cilj je zagotoviti zlasti odpornost, kontinuiteto in razpoložljivost sistemov IKT***, ki podpirajo kritične ali pomembne funkcije,*** ter ohraniti visoke standarde varnosti, zaupnosti in celovitosti podatkov v mirovanju, uporabi ali med prenosom.

3. Za doseganje ciljev iz odstavka 2 finančni subjekti uporabljajo ▌ informacijsko in komunikacijsko tehnologijo in postopke, ki:

   (a) zagotavljajo ***čim večjo*** varnost sredstev za prenos informacij;

   (b) na najmanjšo možno zmanjšujejo tveganje za okvaro ali izgubo podatkov, nepooblaščen dostop in tehnične napake, ki bi lahko oviralo poslovno dejavnost;

(c) preprečujejo uhajanje informacij;

(d) zagotavljajo, da so podatki zaščiteni pred ***notranjimi tveganji na področju IKT, vključno s*** slabim upravljanjem ***in človeškimi napakami***.

4. V sklopu okvira za upravljanje tveganj na področju IKT iz člena 5(1) finančni subjekti ***glede na svoj profil tveganja***:

(a) oblikujejo in dokumentirajo politiko informacijske varnosti, ki določa pravila za zaščito zaupnosti, celovitosti in razpoložljivosti njihovih virov, podatkov in informacijskih sredstev na področju IKT***,*** ter ***poskrbijo za popolno zaščito*** virov, podatkov in informacijskih sredstev na področju IKT pri svojih strankah***, če so sestavni del sistemov IKT finančnega subjekta***;

(b) v skladu s pristopom, ki temelji na tveganju, vzpostavijo zanesljivo upravljanje omrežja in infrastrukture z uporabo ustreznih tehnik, metod in protokolov, ***ki lahko zajemajo izvajanje*** mehanizmov za izolacijo prizadetih informacijskih sredstev v primeru kibernetskih napadov;

(c) izvajajo politike, ***postopke in nadzor,*** ki omejujejo fizični in virtualni dostop do virov in podatkov sistemov IKT na to, kar je potrebno le za zakonite in odobrene funkcije in dejavnosti ;

(d) izvajajo politike in protokole za močne mehanizme avtentikacije ***in zaščito kriptografskih ključev***, ki temeljijo na ustreznih standardih in namenskih nadzornih sistemih ;

(e) izvajajo politike, postopke in kontrole za upravljanje sprememb na področju IKT, vključno s spremembami komponent programske opreme, strojne opreme in strojne programske opreme, sistemskimi ali varnostnimi spremembami, ki temeljijo na pristopu ocene tveganja in so sestavni del celotnega postopka finančnega subjekta za upravljanje sprememb, in sicer za zagotovitev, da se vse spremembe sistemov IKT nadzorovano evidentirajo, testirajo, ocenijo, odobrijo, izvajajo in preverijo;

(f) imajo ustrezne in celovite politike za popravke in posodobitve.

Za namene točke (b) finančni subjekti infrastrukturo omrežnih povezav načrtujejo tako, da je omogočena njena ***čimprejšnja*** prekinitev, in zagotovijo njeno delitev in segmentacijo, da se zmanjša in na najmanjšo možno mero prepreči širjenje negativnih učinkov, zlasti za medsebojno povezane finančne postopke.

Za namene točke (e) postopek upravljanja sprememb na področju IKT odobrijo ustrezne ravni vodstva, in ta postopek ima omogočene tudi posebne protokole za nujne spremembe.

Člen 9

Odkrivanje

1. Finančni subjekti vzpostavijo mehanizme za takojšnje odkrivanje neobičajnega ravnanja v skladu s členom 15, vključno s težavami v zvezi z zmogljivostjo omrežja IKT in incidenti, povezanimi z IKT, ***in če je tehnološko možno, tudi*** za prepoznavanje ***in spremljanje*** vseh morebitnih pomembnih kritičnih točk odpovedi.

Vsi mehanizmi odkrivanja iz prvega pododstavka se redno testirajo v skladu s členom 22.

2. Mehanizmi odkrivanja iz odstavka 1 ***sprožijo postopke*** odkrivanja incidentov, povezanih z IKT, in odzivanja nanje, ***med drugim tudi*** samodejne mehanizme opozarjanja za ustrezne zaposlene, odgovorne za odzivanje na incidente, povezane z IKT.

3. Finančni subjekti ▌namenijo zadostna sredstva in zmogljivosti za spremljanje dejavnosti uporabnikov, pojavov nepravilnega delovanja na področju IKT in incidentov, povezanih z IKT, zlasti kibernetskih napadov.

3a. Finančni subjekti evidentirajo vse incidente, povezane z IKT, ki vplivajo na stabilnost, neprekinjenost ali kakovost finančnih storitev, in sicer tako primere, ko incident dejansko vpliva na te storitve ali ko je verjetno, da bo vplival nanje.

4. Poleg tega finančni subjekti iz točke (l) člena 2(1) vzpostavijo sisteme, s katerimi lahko učinkovito preverijo popolnost poročil o trgovanju, ugotovijo izpuste in očitne napake ter zahtevajo ponovni prenos takih napačnih poročil.

Člen 10

Odzivanje in obnovitev

1. V sklopu okvira za upravljanje tveganj na področju IKT iz člena 5(1) in na podlagi zahtev glede opredelitve iz člena 7 finančni subjekti vzpostavijo ▌celovito politiko neprekinjenega poslovanja na področju IKT, ki ***jo lahko sprejmejo kot ločeno namensko politiko in kot*** sestavni del ***širše in splošne*** operativne politike neprekinjenega poslovanja finančnega subjekta.

   S politiko neprekinjenega poslovanja na področju IKT naj bi finančni subjekti obvladovali in zmanjševali tveganja, ki bi lahko škodljivo vplivala na njihove sisteme IKT in storitve IKT, ter po potrebi olajšali njihovo hitro obnovitev. Finančni subjekti pri oblikovanju politike neprekinjenega poslovanja na področju IKT posebej upoštevajo tveganja, ki bi lahko škodljivo vplivala na storitve IKT in sisteme IKT.

2. Finančni subjekti izvajajo politiko neprekinjenega poslovanja na področju IKT iz odstavka 1 z namenskimi, ustreznimi in dokumentiranimi dogovori, načrti, postopki in mehanizmi, katerih cilj je:

   (b) zagotavljanje neprekinjenosti kritičnih funkcij finančnega subjekta;

   (c) hitro, ustrezno in učinkovito odzivanje na vse incidente, povezane z IKT, med drugim zlasti na kibernetske napade, ter njihovo reševanje, in sicer na način, ki omejuje škodo in daje prednost nadaljevanju dejavnosti in sanacijskim ukrepom;

   (d) takojšnje aktiviranje namenskih načrtov, ki omogočajo zajezitvene ukrepe, postopke in tehnologije, primerne za posamezne vrste incidentov, povezanih z IKT, in preprečevanje nadaljnje škode, ter aktiviranje prilagojenih postopkov odzivanja in okrevanja, določenih v skladu s členom 11;

   (e) ocenjevanje predhodnih učinkov, škode in izgub;

(f) določitev komunikacijskih ukrepov in ukrepov za obvladovanje kriz, ki zagotavljajo, da se posodobljene informacije posredujejo vsem ustreznim internim zaposlenim in zunanjim zainteresiranim stranem v skladu s členom 13 ter da se o njih poroča pristojnim organom v skladu s členom 17.

3. V sklopu okvira za upravljanje tveganj na področju IKT iz člena 5(1) finančni subjekti izvajajo povezan načrt okrevanja IKT po katastrofi, ki je v primeru finančnih subjektov, ki niso mikro podjetja, predmet neodvisnih revizijskih pregledov.

4. Finančni subjekti vzpostavijo, vzdržujejo in redno testirajo ustrezne načrte neprekinjenega poslovanja na področju IKT, zlasti v zvezi s kritičnimi ali pomembnimi funkcijami, oddanimi v zunanje izvajanje ali zagotovljenimi z dogovori s tretjimi ponudniki storitev IKT.

5. V sklopu celovitega upravljanja tveganj na področju IKT finančni subjekti:

(a) testirajo politiko neprekinjenega poslovanja na področju IKT in načrt okrevanja IKT po katastrofi vsaj enkrat letno in po bistvenih spremembah ***kritičnih ali pomembnih*** sistemov IKT;

(b) testirajo načrte obveščanja o kriznih razmerah, vzpostavljene v skladu s členom 13.

Za namene točke (a) finančni subjekti, ki niso mikro podjetja, v načrte testiranja vključijo scenarije kibernetskih napadov in preklopov med primarno infrastrukturo IKT in redundatno zmogljivostjo, rezervnimi sistemi in redundantnimi obrati, potrebnimi za izpolnitev obveznosti iz člena 11.

Finančni subjekti redno pregledujejo svojo politiko neprekinjenega poslovanja na področju IKT in načrt okrevanja IKT po katastrofi, pri čemer upoštevajo rezultate testov, izvedenih v skladu s prvim pododstavkom, in priporočila, ki izhajajo iz revizijskih ali nadzornih pregledov.

6. Finančni subjekti, ki niso mikro podjetja, imajo funkcijo obvladovanja kriz, ***in sicer bodisi kot namensko funkcijo bodisi kot funkcijo, ki vključuje del funkcij s pristojnostmi za odzivanje na incidente in njihovo upravljanje. V*** primeru aktiviranja politike neprekinjenega poslovanja na področju IKT ali načrta okrevanja IKT po katastrofi ***funkcija obvladovanja kriz*** določa jasne postopke za upravljanje notranjih in zunanjih obvestil o kriznih razmerah v skladu s členom 13.

7. Finančni subjekti vodijo evidence o ***ustreznih*** dejavnostih pred motnjami in med njimi, ko se aktivira njihova politika neprekinjenega poslovanja na področju IKT ali načrt okrevanja IKT po katastrofi. Te evidence morajo biti na voljo.

8. Finančni subjekti iz točke (f) člena 2(1) pristojnim organom predložijo kopije rezultatov testov neprekinjenega poslovanja na področju IKT ali podobnih dejavnosti, opravljenih v obdobju pregleda.

9. Finančni subjekti, ki niso mikro podjetja, pristojnim organom poročajo o vseh ***ocenjenih finančnih*** stroških in izgubah, ki nastanejo zaradi ***znatnih*** motenj na področju IKT in ***večjih*** incidentov, povezanih z IKT.

9a. Evropski nadzorni organi prek Skupnega odbora oblikujejo skupne smernice o metodologiji za izračun stroškov in količinsko oceno izgub iz odstavka 9.

Člen 11

Politike varnostnega kopiranja in obnovitvene metode

1. Da bi se zagotovila obnovitev sistemov IKT z minimalnimi izpadi in omejenimi motnjami, finančni subjekti v sklopu okvira za upravljanje tveganj na področju IKT razvijejo:

   (a) politiko varnostnega kopiranja, ki določa obseg podatkov za varnostno kopiranje in najmanjšo pogostost varnostnega kopiranja na podlagi kritičnosti informacij ali občutljivosti podatkov;

   (b) obnovitvene metode.

2. ***V skladu s politiko varnostnega kopiranja iz točke (a) odstavka 1, sistemi*** za varnostno kopiranje začnejo delovati brez nepotrebnega odlašanja, razen če bi tak zagon ogrozil varnost omrežja in informacijskih sistemov ali celovitost ali zaupnost podatkov.

3. Finančni subjekti pri obnavljanju varnostnih kopij podatkov z lastnimi sistemi uporabljajo sisteme IKT, ***ki so bodisi fizično ali logično ločeni od njihovega*** glavnega ***sistema IKT ter niso*** neposredno ***povezani*** z njim in so varno ***zaščiteni*** pred nepooblaščenim dostopom ali okvarami na področju IKT.

   Za finančne subjekte iz točke (g) člena 2(1) morajo načrti okrevanja po katastrofi ob motnji zagotoviti obnovitev vseh transakcij, s čimer bo centralni nasprotni stranki omogočeno zanesljivo nadaljnje delovanje in dokončanje poravnave na predvideni datum.

4. Finančni subjekti ocenijo***, ali je treba vzdrževati*** redundantne zmogljivosti IKT, opremljene z zmogljivosti virov in funkcionalnostmi, ki so zadostne in ustrezne za zagotavljanje poslovnih potreb ***ter izpolnjujejo zahteve glede digitalne operativne odpornosti iz te uredbe***.

5. Finančni subjekti iz točke (f) člena 2(1) skrbijo ali zagotavljajo, da imajo njihovi tretji ponudniki storitev IKT vsaj eno sekundarno lokacijo za obdelavo z viri, zmogljivostmi, funkcionalnostmi in kadrovsko ureditvijo, ki so zadostni in ustrezni za zagotavljanje poslovnih potreb.

   Sekundarna lokacija za obdelavo:

   (a) je na zadostni geografski razdalji od primarne lokacije za obdelavo, da se zagotovi, da ima drugačen profil tveganja, in prepreči, da bi jo prizadel dogodek, ki je prizadel primarno lokacijo;

   (b) je zmožna zagotoviti enako neprekinjenost kritičnih storitev kot na primarni lokaciji ali zagotoviti raven storitev, potrebnih za zagotovitev, da finančni subjekt opravlja svoje kritične operacije v okviru ciljev obnovitve;

   (c) je ▌dostopna zaposlenim pri finančnem subjektu, da se zagotovi neprekinjenost kritičnih ***ali pomembnih funkcij***, če primarna lokacija za obdelavo postane nedostopna.

6. Finančni subjekti pri določanju ciljev glede časa in točk obnovitve za vsako funkcijo upoštevajo***, ali gre za kritično ali pomembno funkcijo,*** in potencialni splošni učinek na učinkovitost trga. Taki cilji glede časa zagotavljajo, da so v skrajnih scenarijih dosežene dogovorjene ravni storitev.

7. Finančni subjekti med obnovitvijo po incidentu, povezanem z IKT, ***poskrbijo za najvišjo*** raven celovitosti podatkov***, na primer z izvajanjem večkratnih pregledov, vključno s postopki usklajevanja***. Ta preverjanja se opravijo tudi pri rekonstrukciji podatkov zunanjih zainteresiranih strani, da se zagotovi skladnost vseh podatkov med sistemi.

Člen 12

Učenje in razvoj

1. Finančni subjekti imajo vzpostavljene zmogljivosti in zaposlene za zbiranje informacij o ranljivostih in kibernetskih grožnjah, incidentih, povezanih z IKT, zlasti kibernetskih napadih, in analizo njihovih verjetnih učinkov na digitalno operativno odpornost finančnih subjektov.

2. Finančni subjekti vzpostavijo preglede po ***večjih*** incidentih, povezanih z IKT, ki se opravijo po večjih motnjah na področju IKT v njihovih osnovnih dejavnostih, s katerimi analizirajo vzroke motnje in opredelijo potrebne izboljšave v delovanju IKT ali politiki neprekinjenega poslovanja na področju IKT iz člena 10.

   Pri izvajanju sprememb ***za obvladovanje tveganj, povezanih z IKT, ki so prepoznana na podlagi pregledov večjih incidentov, povezanih z IKT,*** finančni subjekti, ki niso mikro podjetja, ***vse znatne*** spremembe sporočijo pristojnim organom***, pri čemer podrobno navedejo potrebne izboljšave in kako naj bi v prihodnosti motnje preprečili ali ublažili***. ***Pristojnim organom lahko spremembe sporočijo pred njihovo uvedbo ali po njej.***

   Pri pregledih po incidentih, povezanih z IKT, iz prvega pododstavka se ugotovi, ali so bili upoštevani ustaljeni postopki in ali so bili izvedeni ukrepi učinkoviti, vključno v zvezi s:

   (a) hitrostjo pri odzivanju na varnostna opozorila ter določanju učinka incidentov, povezanih z IKT, in njihove resnosti;

   (b) kakovostjo in hitrostjo izvedbe forenzične analize;

   (c) učinkovitostjo prenosa incidenta na višjo raven v finančnem subjektu;

   (d) učinkovitostjo notranje in zunanje komunikacije.

3. Spoznanja, pridobljena pri testiranju digitalne operativne odpornosti, izvedenem v skladu s členoma 23 in 24, in pri resničnih incidentih, povezanih z IKT, zlasti kibernetskih napadih, se skupaj z izzivi, ki se pojavljajo pri aktivaciji načrta neprekinjenega poslovanja ali načrta okrevanja po katastrofi, ter ustreznimi informacijami, izmenjanimi z nasprotnimi strankami in ocenjenimi med nadzornimi pregledi, stalno vključujejo v postopek ocene tveganj na področju IKT. Te ugotovitve se pretvorijo v ustrezne preglede zadevnih komponent okvira za upravljanje tveganj na področju IKT iz člena 5(1).

4. Finančni subjekti spremljajo učinkovitost izvajanja svoje strategije za digitalno odpornost iz člena 5(9). Popišejo razvoj tveganj na področju IKT skozi čas***, med drugim tudi, koliko se ta tveganja približajo kritičnim ali pomembnim funkcijam,*** analizirajo pogostost, vrste, obseg in razvoj incidentov, povezanih z IKT, zlasti kibernetskih napadov in njihovih vzorcev, da bi razumeli stopnjo izpostavljenosti tveganju na

področju IKT ter okrepili kibernetsko zrelost in pripravljenost finančnega subjekta.

5. Višji uslužbenci na področju IKT vsaj enkrat letno poročajo upravljalnemu organu o ugotovitvah iz odstavka 3 in podajo priporočila.

6. Finančni subjekti oblikujejo programe ozaveščanja o varnosti IKT in usposabljanja na področju digitalne operativne odpornosti kot obvezne module v svojih shemah za usposabljanje osebja. ***Programi ozaveščanja o varnosti IKT se izvajajo za vse osebje. Usposabljanje o digitalni operativni odpornosti se izvajajo vsaj*** za vse zaposlene***, ki imajo pravice neposrednega dostopa do sistemov IKT,*** in za višje vodstvene delavce. ***Zahtevnost modulov usposabljanja je sorazmerna z ravnjo neposrednega dostopa člana osebja do sistemov IKT, pri čemer se upošteva zlasti dostop do kritičnih ali pomembnih funkcij.***

   Finančni subjekti***, ki niso mikro podjetja,*** stalno spremljajo ustrezne tehnološke trende, tudi zato, da bi razumeli možne učinke uvajanja takih novih tehnologij na zahteve za varnost IKT in digitalno operativno odpornost. Seznanjeni so z najnovejšimi postopki upravljanja tveganj na področju IKT in učinkovito preprečujejo sedanje ali nove oblike kibernetskih napadov.

Člen 13

Obveščanje

1. V sklopu okvira za upravljanje tveganj na področju IKT iz člena 5(1) finančni subjekti pripravijo načrte obveščanja, ki omogočajo ***vsaj*** odgovorno razkritje ***večjih*** incidentov ali večjih ranljivosti, povezanih z IKT, strankam in partnerjem ter javnosti, kjer je to ustrezno.

   V načrtih obveščanja iz prvega pododstavka tudi zagotovijo, da se strankam in partnerjem vsako leto razkrije povzetek vseh incidentov, povezanih z IKT. Pri tem se popolnoma spoštuje poslovna zaupnost finančnega subjekta ter njegovih strank in partnerjev ter se ne ogroža okvir za upravljanje tveganj na področju IKT iz člena 5(1).

2. V sklopu okvira za upravljanje tveganj na področju IKT iz člena 5(1) finančni subjekti izvajajo komunikacijske politike za zaposlene in zunanje zainteresirane strani. Komunikacijske politike za zaposlene upoštevajo potrebo po razlikovanju med zaposlenimi, ki sodelujejo pri upravljanju tveganj na področju IKT, zlasti pri odzivanju in obnovitvi, ter zaposlenimi, ki jih je treba obvestiti.

3. Vsaj ena oseba pri subjektu je odgovorna za izvajanje strategije obveščanja ***vsaj*** za ***večje*** incidente, povezane z IKT, in v ta namen opravlja vlogo predstavnika za stike z javnostjo in mediji.

Člen 14

Nadaljnje usklajevanje orodij, metod, postopkov in politik za upravljanje tveganj na področju IKT

Evropski bančni organ (EBA), Evropski organ za vrednostne papirje in trge (ESMA) ter Evropski organ za zavarovanja in poklicne pokojnine (EIOPA) v posvetovanju z Agencijo Evropske unije za kibernetsko varnost (ENISA) pripravijo osnutke regulativnih tehničnih standardov za naslednje namene:

(a) določitev nadaljnjih elementov, ki jih je treba vključiti v varnostne politike, postopke, protokole in orodja IKT iz člena 8(2), da bi se zagotovila varnost omrežij, omogočili ustrezni zaščitni ukrepi pred vdori in zlorabo podatkov, ohranili pristnost in celovitost podatkov, vključno z uporabo kriptografskih tehnik, ter zagotovil natančen in hiter prenos podatkov brez večjih motenj ***in nepotrebnih zamud***;

(d) razvoj nadaljnjih komponent za nadzor pravic upravljanja dostopa iz točke (c) člena 8(4) in s tem povezane kadrovske politike, ki določajo pravice dostopa ter postopke za podeljevanje in odvzem pravic ter spremljanje neobičajnega ravnanja v zvezi s tveganji na področju IKT z ustreznimi kazalniki, tudi za vzorce uporabe omrežja, ure, dejavnost IT in neznane naprave;

(e) nadaljnji razvoj elementov iz člena 9(1), ki omogočajo takojšnje odkrivanje neobičajnega ravnanja, in meril iz člena 9(2), ki sprožijo postopke odkrivanja incidentov, povezanih z IKT, in odzivanja nanje;

(f) nadaljnja opredelitev komponent politike neprekinjenega poslovanja na področju IKT iz člena 10 (1);

(g) nadaljnja opredelitev testiranja načrtov neprekinjenega poslovanja na področju IKT iz člena 10(5), da se zagotovi ustrezno upoštevanje scenarijev, v katerih kakovost zagotavljanja kritične ali pomembne funkcije pade na nesprejemljivo raven ali povsem odpove, in ustrezno upošteva potencialni vpliv plačilne nesposobnosti ali drugega prenehanja delovanja katerega koli zadevnega tretjega ponudnika storitev IKT in, kjer je to ustrezno, politična tveganja v jurisdikcijah teh ponudnikov;

(h) nadaljnja opredelitev komponent načrta okrevanja IKT po katastrofi iz člena 10(3).

Evropski nadzorni organi te osnutke regulativnih tehničnih standardov Komisiji predložijo do [UP: vstaviti datum eno leto po datumu začetka veljavnosti].

Na Komisijo se prenese pooblastilo za sprejetje regulativnih tehničnih standardov iz prvega pododstavka v skladu s členi 10 do 14 Uredbe (EU) št. 1093/2010, (EU) št. 1094/2010 oziroma (EU) št. 1095/2010.

Člen 14a

Okvir za upravljanje tveganj na področju IKT za male, nepovezane in izvzete subjekte

1. V skladu s členom 3a mala in nepovezana investicijska podjetja, plačilne institucije, izvzete z Direktivo (EU) 2015/2366, kreditne institucije, izvzete z Direktivo 2013/36/EU, institucije za izdajo elektronskega denarja, izvzete z Direktivo 2009/110/ES, in male institucije za poklicne pokojninske pokojnine vzpostavijo in vzdržujejo zanesljiv in dokumentiran okvir za upravljanje tveganj na področju IKT, s katerim:

(a) podrobno določijo mehanizme in ukrepe za hitro, učinkovito in celovito upravljanje vseh tveganj na področju IKT, vključno z zaščito ustreznih fizičnih komponent in infrastrukture;

(b) stalno preverjajo varnost in delovanje vseh sistemov IKT;

(c) čim bolj zmanjšajo vpliv tveganj na področju IKT, in sicer z uporabo

zanesljivih, odpornih in posodobljenih sistemov, protokolov in orodij IKT, ki so primerni za podporo izvajanju njihovih dejavnosti in zagotavljanju storitev;

(d) ustrezno varujejo zaupnost, celovitost in razpoložljivost podatkovnih omrežij in informacijskih sistemov;

(e) omogočijo hitro prepoznavanje in odkrivanje virov tveganja in nepravilnosti v omrežju in informacijskih sistemih ter hitro obravnavo incidentov na področju IKT.

2. Okvir za upravljanje tveganj na področju IKT iz odstavka 1 se dokumentira in pregleda najmanj enkrat letno, pa tudi ob pojavu večjih incidentov, povezanih z IKT, pri čemer se upoštevajo nadzorna navodila ali sklepi, ki izhajajo iz ustreznih postopkov testiranja ali revizije digitalne operativne odpornosti. Okvir se nenehno izpopolnjuje na podlagi izkušenj, pridobljenih pri izvajanju in spremljanju.

Poročilo o pregledu okvira za upravljanje tveganj na področju IKT se vsako leto predloži pristojnemu organu.

POGLAVJE III

INCIDENTI, POVEZANI Z IKT

UPRAVLJANJE, RAZVRŠČANJE in POROČANJE

Člen 15

Postopek upravljanja incidentov, povezanih z IKT

1. Finančni subjekti vzpostavijo in izvajajo postopek upravljanja incidentov, povezanih z IKT, za odkrivanje, upravljanje in obveščanje o incidentih, povezanih z IKT, ter vzpostavijo kazalnike za zgodnje opozarjanje kot opozorila.

2. Finančni subjekti vzpostavijo ustrezne postopke ***in procese*** za zagotovitev doslednega in celovitega spremljanja, obravnavanja in nadaljnjega spremljanja incidentov, povezanih z IKT, da se zagotovi prepoznavanje in ***obravnavanje*** temeljnih vzrokov ter s tem prepreči pojavljanje tovrstnih incidentov.

3. V postopku upravljanja incidentov, povezanih z IKT, iz odstavka 1 se:

   (a) vzpostavijo postopki za opredelitev, sledenje, evidentiranje, kategoriziranje in razvrščanje incidentov, povezanih z IKT, glede na njihovo prioriteto ter resnost in kritičnost prizadetih storitev v skladu z merili iz člena 16(1);

   (b) dodelijo vloge in odgovornosti, ki jih je treba aktivirati za različne vrste in scenarije incidentov, povezanih z IKT;

   (c) določijo načrti za obveščanje zaposlenih, zunanjih zainteresiranih strani in medijev v skladu s členom 13 ter za obveščanje strank, za postopke notranjega prenosa na višjo raven, vključno s pritožbami strank v zvezi z IKT, ter za zagotavljanje informacij finančnim subjektom, ki delujejo kot partnerji, kot je ustrezno;

   (d) zagotovi, da se ***vsaj*** o večjih incidentih, povezanih z IKT, poroča ustreznim višjim vodstvenim delavcem, in o večjih incidentih, povezanih z IKT, obvesti upravljalni organ, pri čemer se pojasnijo učinek, odziv in dodatne kontrole, ki jih je treba vzpostaviti zaradi ***večjih*** incidentov, povezanih z IKT;

   (e) vzpostavijo postopki odzivanja na incidente, povezane z IKT, za zmanjšanje njihovih učinkov in zagotovitev, da začnejo storitve delovati pravočasno in varno.

Člen 16

Razvrščanje incidentov, povezanih z IKT

1. Finančni subjekti razvrstijo incidente, povezane z IKT, in določijo njihov učinek na podlagi naslednjih meril:

   (a) število uporabnikov ali finančnih partnerjev, ki jih je prizadela motnja zaradi incidenta, povezanega z IKT ▌;

(b) trajanje incidenta, povezanega z IKT, vključno z nedelovanjem storitve;

(c) geografska razpršenost območij, ki jih je prizadel incident, povezan z IKT, zlasti če prizadene več kot dve državi članici;

(d) izgube podatkov, ki jih povzroči incident, povezan z IKT, kot so izguba celovitosti, izguba zaupnosti ali izguba razpoložljivosti;

(e) resnost učinka incidenta, povezanega z IKT, na sisteme IKT finančnega subjekta;

(f) kritičnost prizadetih storitev, vključno s transakcijami in poslovanjem finančnega subjekta;

(g) gospodarski učinek incidenta, povezanega z IKT, v absolutnem in relativnem smislu.

2. Evropski nadzorni organi prek Skupnega odbora evropskih nadzornih organov (v nadaljnjem besedilu: Skupni odbor) in ***v sodelovanju*** z Evropsko centralno banko (ECB) in ENISA pripravijo skupne osnutke regulativnih tehničnih standardov, ki podrobneje določajo:

(a) merila iz odstavka 1, vključno s pragovi pomembnosti za določanje večjih incidentov, povezanih z IKT, za katere velja obveznost poročanja iz člena 17(1);

(b) merila, ki jih pristojni organi uporabijo za oceno pomena večjih incidentov, povezanih z IKT, za jurisdikcije v drugih državah članicah, in podrobnosti poročil o ***večjih*** incidentih, povezanih z IKT, ki jih je treba deliti z drugimi pristojnimi organi v skladu s točkama 5 in 6 člena 17.

3. Evropski nadzorni organi pri razvoju skupnih osnutkov regulativnih tehničnih standardov iz odstavka 2 upoštevajo mednarodne standarde ter specifikacije, ki jih je razvila in objavila agencija ENISA, vključno s specifikacijami za druge gospodarske sektorje, kjer je to ustrezno. ***Poleg tega evropski nadzorni organi upoštevajo, da mala in mikro podjetja pri pravočasnem in učinkovitem obvladovanju incidenta niso omejena z zahtevo po spoštovanju klasifikacijskih zahtev iz tega člena. Evropski nadzorni organi upoštevajo tudi velikost finančnih subjektov, naravo, obseg in kompleksnost njihovih storitev, dejavnosti in poslovanja ter njihov splošni profil tveganja.***

Evropski nadzorni organi te skupne osnutke regulativnih tehničnih standardov predložijo Komisiji do [UP: vstaviti datum ***dve leti*** po datumu začetka veljavnosti].

Na Komisijo se prenese pooblastilo za dopolnitev te uredbe s sprejetjem regulativnih tehničnih standardov iz odstavka 2 v skladu s členi 10 do 14 Uredbe (EU) št. 1093/2010, (EU) št. 1094/2010 oziroma (EU) št. 1095/2010.

Člen 17

Poročanje o večjih incidentih, povezanih z IKT

1. Finančni subjekti o večjih incidentih, povezanih z IKT, poročajo ustreznemu pristojnemu organu iz člena 41 v rokih, določenih v odstavku 3.

Za namene prvega pododstavka finančni subjekti po zbiranju in analizi vseh ustreznih informacij pripravijo poročilo o incidentu z uporabo predloge iz člena 18 in ga

posredujejo pristojnemu organu.

Poročilo vključuje vse informacije, ki so potrebne, da pristojni organ določi pomen večjega incidenta, povezanega z IKT, in oceni možne čezmejne učinke.

1a. Finančni subjekti lahko o znatnih kibernetskih grožnjah prostovoljno obvestijo ustrezni pristojni organ, če menijo, da je grožnja relevantna za finančni sistem, uporabnike storitev ali stranke. Pristojni organ lahko te informacije posreduje drugim ustreznim organom v skladu z odstavkom 5.

2. Kadar ***pride do večjega incidenta***, ***povezanega*** z IKT, ***in ta pomembno*** vpliva ▌ na finančne interese uporabnikov storitev in strank, finančni subjekti uporabnike svojih storitev in stranke ▌ o tem incidentu seznanijo ***takoj, ko izvedo zanj,*** in jih ▌ obvestijo o vseh ***ustreznih*** ukrepih, ki so bili sprejeti za zmanjšanje njegovih škodljivih učinkov. ***Če zaradi protiukrepov, ki jih sprejme finančni subjekt, uporabniki storitev in stranke ne utrpijo škode, zahteva po obveščanju uporabnikov storitev in strank ne velja.***

3. Finančni subjekti pristojnemu organu iz člena 41 predložijo:

(a) začetno obvestilo ***o večjem incidentu, povezanem*** z IKT, ***ki vsebuje informacije, ki jih je priglasitelj pridobil po najboljših močeh, kot sledi***:

(i) pristojni organ je treba nemudoma, v vsakem primeru pa v 24 urah po seznanitvi z incidentom, obvestiti o incidentih, ki povzročijo znatno motnjo v razpoložljivosti storitev, ki jih zagotavlja finančni subjekt;

(ii) pristojni organ je treba nemudoma, v vsakem primeru pa v 72 urah po seznanitvi z incidentom, obvestiti o incidentih, ki znatno vplivajo na finančni subjekt, vendar ne na razpoložljivost storitev, ki jih zagotavlja;

(iii) pristojni organ je treba nemudoma, v vsakem primeru pa v 24 urah po seznanitvi z incidentom, obvestiti o incidentih, ki vplivajo na celovitost, zaupnost ali varnost osebnih podatkov, ki jih vzdržuje finančni subjekt;

(b) vmesno poročilo***, in sicer ga predložijo takoj, ko se status prvotnega incidenta bistveno spremeni ali ko se pojavijo nove informacije, ki bi lahko znatno vplivale na to, kako pristojni organ obravnava incident, povezan z IKT, ter*** po začetnem obvestilu iz točke (a), temu pa vsakič, ko je na voljo ustrezna posodobitev statusa, ali na posebno zahtevo pristojnega organa predložijo ustrezna posodobljena obvestila;

(c) končno poročilo, ko je končana analiza osnovnega vzroka, ne glede na to, ali so bili ukrepi za ublažitev že izvedeni ali ne, in ko so na voljo podatki o dejanskem učinku, ki nadomeščajo ocene, vendar najpozneje en mesec od ***datuma*** oddaje začetnega poročila;

(ca) če je incident ob roku za predložitev končnega poročila iz točke (c) incident še vedno prisoten, se končno poročilo predloži en mesec po njegovi odpravi.

Ustrezni pristojni organ iz člena 41 poskrbi, da lahko finančni subjekt v ustrezno utemeljenih primerih odstopa od rokov iz točk (a), (b), (c) in (ca) tega odstavka, pri čemer upošteva, ali finančni subjekti v zvezi z večjimi incidenti, povezanimi z IKT, lahko predložijo točne in smiselne informacije.

4. Finančni subjekti lahko prenesejo obveznosti poročanja iz tega člena na tretjega

ponudnika storitev le z odobritvijo takega prenosa s strani ustreznega pristojnega organa iz člena 41. ***V teh primerih finančni subjekt ostane v celoti odgovoren za izpolnjevanje zahtev glede poročanja o incidentih.***

5. Pristojni organ po prejemu poročila iz odstavka 1 brez nepotrebnega odlašanja sporoči podrobnosti o ***večjem*** incidentu***, povezanem z IKT,*** naslednjim institucijam:

(a) EBA, ESMA ali EIOPA, kot je ustrezno;

(b) ECB, kot je ustrezno, za finančne subjekte iz točk (a), (b) in (c) člena 2(1), in

(c) enotni kontaktni točki, določeni v skladu s členom 8 Direktive (EU) 2016/1148***, ali nacionalnim skupinam za odzivanje na incidente na področju računalniške varnosti, imenovanim na podlagi člena 9 Direktive (EU) 2016/1149****;*

(ca) organu za reševanje, pristojnemu za zadevni finančni subjekt. Enotnemu odboru za reševanje (SRB) v zvezi s subjekti iz člena 7(2) Uredbe (EU) št. 806/2014 ter subjekti in skupinami iz člena 7(4)(b) in (5) Uredbe (EU) št. 806/2014, kadar so izpolnjeni pogoji za uporabo navedenih odstavkov;

(cb) nacionalnim organom za reševanje, v zvezi s subjekti in skupinami iz člena 7(3) Uredbe (EU) št. 806/2014. Nacionalni organi za reševanje Enotnemu odboru za reševanje vsako četrtletje predložijo povzetek poročil, ki so jih prejeli v skladu s to točko v zvezi s subjekti in skupinami iz člena 7(3) Uredbe (EU) št. 806/2014;

(cc) drugim ustreznim javnim organom, tudi v drugih državah članicah.

6. EBA, ESMA ali EIOPA in ECB v ***sodelovanju z ENISA*** ocenijo pomen večjega incidenta, povezanega z IKT, za druge ustrezne javne organe in jih o tem čim prej obvestijo. ECB člane Evropskega sistema centralnih bank obvesti o zadevah, pomembnih za plačilni sistem. Pristojni organi na podlagi obvestila, kadar je ustrezno, sprejmejo vse potrebne ukrepe za zagotovitev takojšnje stabilnosti finančnega sistema.

Člen 18

Usklajevanje vsebine in predlog za poročanje

1. Evropski nadzorni organi prek Skupnega odbora in po posvetovanju z ENISA in ECB razvijejo:

(a) skupne osnutke regulativnih tehničnih standardov, da:

(1) določijo vsebino poročanja o večjih incidentih, povezanih z IKT;

(2) nadalje opredelijo pogoje, pod katerimi lahko finančni subjekti s predhodno odobritvijo pristojnega organa prenesejo obveznosti poročanja iz tega poglavja na tretjega ponudnika storitev;

(3) podrobneje določijo merila za oceno vpliva večjega incidenta, povezanega z IKT, na finančni subjekt za namene člena 17(3)(a).

(b) skupne osnutke izvedbenih tehničnih standardov, da vzpostavijo standardne

obrazce, predloge in postopke, v okviru katerih finančni subjekti poročajo o večjem incidentu, povezanem z IKT.

Evropski nadzorni organi skupne osnutke regulativnih tehničnih standardov iz točke (a) ***prvega pododstavka*** in skupne osnutke izvedbenih tehničnih standardov iz točke (b) ***prvega pododstavka*** predložijo Komisiji do xx 202x [UP: vstaviti datum ***dve leti*** po datumu začetka veljavnosti].

Na Komisijo se prenese pooblastilo za dopolnitev te uredbe s sprejetjem skupnih regulativnih tehničnih standardov iz točke (a) ***prvega pododstavka*** v skladu s členi 10 do 14 Uredbe (EU) št. 1093/2010, (EU) št. 1095/2010 oziroma (EU) št. 1094/2010.

Na Komisijo se prenese pooblastilo za sprejetje skupnih izvedbenih tehničnih standardov iz točke (b) ***prvega pododstavka*** v skladu s členom 15 Uredbe (EU) št. 1093/2010, (EU) št. 1095/2010 oziroma (EU) št. 1094/2010.

2. Dokler niso na voljo rezultati poročila o izvedljivosti iz člena 19 o nadaljnji centralizaciji poročanja o incidentih, evropski nadzorni organi prek skupnega odbora in v sodelovanju s pristojnimi organi, ECB, Enotnim odborom za reševanje in ENISA pripravijo smernice za izmenjavo informacij o poročilih o večjih incidentih, povezanih z IKT, v skladu s členom 17(5).

V smernicah iz prvega pododstavka upoštevajo vsaj naslednje:

(a) najučinkovitejše komunikacijske poti;

(b) vzdrževanje varnosti, zaupnosti in celovitosti podatkov, ki se izmenjujejo;

(c) morebitno vključitev finančnih subjektov za dopolnitev izmenjave informacij iz člena 40.

Člen 19

Centralizacija poročanja o večjih incidentih, povezanih z IKT

1. Evropski nadzorni organi prek Skupnega odbora in po posvetovanju z ECB in ENISA pripravijo skupno poročilo, v katerem ocenijo izvedljivost nadaljnje centralizacije poročanja o incidentih z vzpostavitvijo enotnega vozlišča EU, kjer lahko finančni subjekti poročajo o večjih incidentih, povezanih z IKT. V poročilu se preuči, kako olajšati pretok poročanja o incidentih, povezanih z IKT, znižati s tem povezane stroške in podpirati tematske analize za povečanje konvergence nadzora.

2. Poročilo iz odstavka 1 vsebuje vsaj naslednje elemente:

(a) pogoje za vzpostavitev ***enotnega*** vozlišča EU;

(b) koristi, omejitve in možna tveganja;

(ba) zmožnost vzpostavitve interoperabilnosti in ocene njene dodane vrednosti glede na druge upoštevne sheme poročanja, vključno z Direktivo (EU) 2016/1148;

(c) elemente operativnega upravljanja;

(d) pogoje članstva;

(e) načine, na katere lahko finančni subjekti in pristojni organi dostopajo do

enotnega vozlišča EU;

(f) predhodno oceno finančnih stroškov, povezanih z vzpostavitvijo operativne platforme za podporo ***enotnega*** vozlišču EU, vključno z zahtevanim strokovnim znanjem.

3. Evropski nadzorni organi poročilo iz odstavka 1 predložijo Komisiji, Evropskemu parlamentu in Svetu do xx 202x [UL: vstaviti datum tri leta po datumu začetka veljavnosti].

Člen 20

Povratne informacije nadzornih organov

1. Po prejemu poročila iz člena 17(1) pristojni organ potrdi prejem obvestila in finančnemu subjektu čim prej zagotovi vse potrebne povratne informacije ali smernice, zlasti za razpravo o popravnih ukrepih na ravni subjekta ali načinih za zmanjšanje škodljivih učinkov v posameznih sektorjih na najmanjšo možno mero***, ter vsem zadevnim finančnim subjektom, kadar bi to lahko bilo koristno, zagotovi ustrezno anonimizirane povratne informacije, vpogled in obveščevalne podatke, in sicer na podlagi vseh poročil o večjih incidentih, povezanih z IKT, ki jih prejme***.

2. Evropski nadzorni organi prek Skupnega odbora enkrat letno na anonimizirani in združeni podlagi poročajo o obvestilih o ***večjih*** incidentih, povezanih z IKT, ki jih prejmejo pristojni organi, pri čemer navedejo vsaj število večjih incidentov, povezanih z IKT, njihovo naravo, učinek na poslovanje finančnih subjektov ali strank, ***ocenjene*** stroške in izvedene popravne ukrepe.

Evropski nadzorni organi izdajo opozorila in pripravijo statistične podatke na visoki ravni v podporo ocenam groženj in ranljivosti na področju IKT.

Člen 20a

S plačili povezani operativni ali varnostni incidenti, ki zadevajo nekatere finančne subjekte

Zahteve iz tega poglavja se uporabljajo tudi za operativne ali varnostne incidente, povezane s plačili, in večje tovrstne incidente, kadar zadevajo finančne subjekte iz točk (a), (b) in (c) člena 2(1).

POGLAVJE IV

TESTIRANJE DIGITALNE OPERATIVNE ODPORNOSTI

Člen 21

Splošne zahteve za izvajanje testiranja digitalne operativne odpornosti

1. Finančni subjekti***, ki niso mikro podjetja,*** za namene ocenjevanja pripravljenosti na incidente, povezane z IKT, ugotavljanja slabosti, pomanjkljivosti ali vrzeli v digitalni operativni odpornosti in takojšnjega izvajanja popravnih ukrepov vzpostavijo, vzdržujejo in pregledujejo trden in celovit program za testiranje digitalne operativne odpornosti v sklopu okvira za upravljanje tveganj na področju IKT iz člena 5 ▌.

2. Program za testiranje digitalne operativne odpornosti vključuje vrsto ocen, testov, metodologij, praks in orodij, ki se uporabljajo v skladu z določbami členov 22 in 23.

3. Finančni subjekti pri izvajanju programa za testiranje digitalne operativne odpornosti iz odstavka 1 sledijo pristopu, ki temelji na tveganju, pri čemer upoštevajo spreminjajočo se krajino tveganj na področju IKT, morebitna posebna tveganja, ki jim je finančni subjekt izpostavljen ali bi lahko bil izpostavljen, kritičnost informacijskih sredstev in storitev, ki se zagotavljajo, ter vse druge dejavnike, ki se finančnemu subjektu zdijo ustrezni.

4. Finančni subjekti zagotovijo, da teste izvajajo notranje ali zunanje neodvisne strani. ***Kadar teste izvajajo notranji preizkuševalci, finančni subjekti temu namenijo zadostna sredstva in zagotovijo, da se v fazi zasnove in izvedbe testa prepreči nasprotje interesov.***

5. Finančni subjekti vzpostavijo postopke in politike za prednostno obravnavo, razvrstitev in ***odpravljanje*** vseh težav, ki so bile ugotovljene med izvajanjem testov, ter vzpostavijo notranje metodologije za validacijo, da ugotovijo, ali so v celoti obravnavane vse ugotovljene slabosti, pomanjkljivosti ali vrzeli.

6. Finančni subjekti ***poskrbijo, da se*** vsaj enkrat letno ustrezno testirajo ***vsi kritični sistemi*** in aplikacije IKT.

Člen 22

Testiranje sistemov in orodij IKT

1. Program za testiranje digitalne operativne odpornosti iz člena 21 zagotavlja izvajanje celotnega sklopa ustreznih testov**.**

Ti testi lahko vključujejo ocene in ***preglede*** ranljivosti, ***analize*** odprtokodne programske opreme, ***ocene*** varnosti omrežja, ***analize*** vrzeli, ***preglede*** fizične varnosti, ***vprašalnike*** in ***rešitve*** za preiskovanje programske opreme, ***preglede*** izvorne kode, kjer je to mogoče, ***testiranje*** na podlagi scenarijev, ***teste*** združljivosti, ***teste*** učinkovitosti, ***celovito testiranje*** ali ***penetracijsko testiranje***.

2. Finančni subjekti iz točk (f) in (g) člena 2(1) izvedejo ocene ranljivosti pred kakršno koli uvedbo ali prerazporeditvijo novih ali obstoječih storitev, ki podpirajo kritične funkcije, aplikacije in infrastrukturne komponente finančnega subjekta.

Člen 23

Napredno testiranje orodij, sistemov in postopkov IKT na podlagi penetracijskega testiranja na podlagi analize groženj

1. Finančni subjekti, opredeljeni v skladu z ***drugim pododstavkom odstavka*** 3, vsaj vsaka tri leta izvedejo napredno penetracijsko testiranje na podlagi analize groženj.

2. Penetracijsko testiranje na podlagi analize groženj zajema vsaj kritične ***ali pomembne*** funkcije in storitve finančnega subjekta ter se izvaja na aktivnih produkcijskih sistemih, ki podpirajo te funkcije***, kadar je to mogoče, in na predprodukcijskih sistemih z enako varnostno konfiguracijo***. Natančen obseg penetracijskega testiranja na podlagi analize groženj, ki temelji na oceni kritičnih ***ali pomembnih*** funkcij in storitev, določijo finančni subjekti in potrdijo pristojni organi. Ne zahteva se, da en sam penetracijski test na podlagi analize groženj zajame vse kritične ali pomembne funkcije.

   Za namene prvega pododstavka finančni subjekti opredelijo vse ustrezne osnovne postopke, sisteme in tehnologije IKT, ki podpirajo kritične ***ali pomembne*** funkcije in storitve, vključno s ***kritičnimi ali pomembnimi*** funkcijami in storitvami, ki so oddane v izvajanje ali zunanje izvajanje tretjim ponudnikom storitev IKT.

   Kadar so v penetracijsko testiranje na podlagi analize groženj vključeni ***ključni*** tretji ponudniki storitev IKT ***in po potrebi neključni tretji ponudniki storitev IKT***, finančni subjekt sprejme potrebne ukrepe, da zagotovi sodelovanje teh ponudnikov. ***Ti tretji ponudniki storitev IKT niso dolžni sporočiti informacij ali kakršnih koli podrobnosti v zvezi s zadevami, ki niso relevantne za nadzor upravljanja tveganj v zvezi z zadevnimi kritičnimi ali pomembnimi funkcijami finančnih subjektov. To testiranje ne sme negativno vplivati na druge stranke tretjih ponudnikov storitev IKT.***

   Kadar bi lahko udeležba tretjega ponudnika storitev IKT v penetracijskem testiranju na podlagi analize groženj vplivala na kakovost, zaupnost ali varnost njegovih storitev za druge stranke, ki niso zajete v področje uporabe te uredbe, ali na splošno celovitost njegovih operacij, se lahko finančni subjekt in tretji ponudnik storitev IKT pogodbeno dogovorita, da lahko slednji sklene pogodbene dogovore neposredno z zunanjim preizkuševalcem. Za izvajanje skupnega testiranja lahko tretji ponudniki storitev IKT tovrstne dogovore sklenejo v imenu vseh svojih strank, ki so finančni subjekti.

   Finančni subjekti uporabljajo učinkovite kontrole za upravljanje tveganj, da zmanjšajo tveganja morebitnega učinka na podatke, škode na sredstvih in motenj v kritičnih ***ali pomembnih funkcijah*** ali poslovanju samega finančnega subjekta, njegovih nasprotnih strank ali v finančnem sektorju.

   Na koncu testiranja, po dogovoru glede poročil in sanacijskih načrtov, finančni subjekt in zunanji preizkuševalci ***enotnemu javnemu*** organu***, imenovanemu na podlagi odstavka 3a, ali, v primeru, da tretji ponudnik storitev IKT sklene pogodbene dogovore neposredno z zunanjimi preizkuševalci, ENISA predložijo zaupni povzetek rezultatov testiranja in*** dokumentacijo, ki potrjuje, da je bilo penetracijsko testiranje na podlagi analize groženj izvedeno v skladu z zahtevami. ***Enotni javni organ ali ENISA, kakor je ustrezno, izda*** potrdilo***, da je bilo testiranje izvedeno v skladu z zahtevami iz dokumentacije, da bi lahko pristojni organi penetracijsko testiranje na podlagi analize groženj vzajemno priznali***. ***Potrdilo se posreduje pristojnim organom finančnega subjekta in po potrebi glavnemu nadzorniku ključnega tretjega***

ponudnika storitev IKT.

3. Finančni subjekti ***ali tretji ponudniki storitev IKT, ki imajo dovoljenje za sklepanje pogodbenih dogovorov neposredno z zunanjim preizkuševalcem v skladu z odstavkom 2 tega člena,*** sklenejo pogodbo s preizkuševalci v skladu s členom 24 za namene izvajanja penetracijskega testiranja na podlagi analize groženj.

Pristojni organi **–** ***brez poseganja v njihovo pravico, da naloge in pristojnosti iz tega člena prenesejo na druge pristojne organe, odgovorne za penetracijsko testiranje na podlagi analize groženj –,*** finančne subjekte, ki naj bi izvedli penetracijsko testiranje na podlagi analize groženj, določijo na sorazmeren način ▌ na podlagi ocene:

(a) dejavnikov, povezanih z učinki, zlasti kritičnosti zagotovljenih storitev in dejavnosti, ki jih izvaja finančni subjekt;

(b) morebitnih pomislekov glede finančne stabilnosti, vključno s sistemskim značajem finančnega subjekta na nacionalni ravni ali ravni Unije, kot je ustrezno;

(c) posebnega profila tveganja na področju IKT, stopnje zrelosti finančnega subjekta na področju IKT ali značilnosti vključene tehnologije.

3a Države članice imenujejo en sam javni organ, ki je odgovoren za penetracijsko testiranje na podlagi groženj v finančnem sektorju na nacionalni ravni, razen za določitev finančnih subjektov v skladu z odstavkom 3, vključno s penetracijskim testiranjem na podlagi groženj, ki ga izvajajo finančni subjekti in tretji ponudniki storitev IKT, ki sklenejo pogodbene dogovore neposredno z zunanjimi preizkuševalci. Imenovani enotni javni organ ima vse pristojnosti in naloge, potrebne za ta namen.

4. ***Evropski nadzorni organi ob usklajevanju*** z ECB in ob upoštevanju ustreznih okvirov v Uniji, ki veljajo za penetracijsko testiranje na podlagi ***analize groženj, ki se izvede s pomočjo*** obveščevalnih podatkov, ***vključno z okvirom TIBER-EU,*** pripravijo ***sklop osnutkov*** regulativnih tehničnih standardov, v katerih podrobneje določijo:

(a) merila, ki veljajo za namene uporabe ***drugega pododstavka*** odstavka ***3*** tega člena;

(b) zahteve v zvezi z:

(i) obsegom penetracijskega testiranja na podlagi analize groženj iz odstavka 2 tega člena;

(ii) metodologijo in pristopom testiranja, ki ju je treba upoštevati za vsako posamezno fazo testiranja;

(iii) rezultati ter zaključno fazo in fazo sanacije;

(c) vrsto sodelovanja nadzornih organov, ki je potrebno za izvedbo ***in lažje polno medsebojno priznavanje*** penetracijskega testiranja na podlagi analize groženj pri finančnih subjektih, ki delujejo v več kot eni državi članici, ***in testiranj, ki jih opravijo zunanji preizkuševalci, ki so pogodbene dogovore sklenili neposredno s tretjimi ponudniki storitev IKT v skladu z drugim odstavkom tega člena,*** da se omogoči ustrezna raven sodelovanja nadzornih organov in prilagodljivo izvajanje z upoštevanjem posebnosti finančnih podsektorjev ali lokalnih finančnih trgov.

Evropski nadzorni organi te osnutke regulativnih tehničnih standardov Komisiji predložijo do [UL: vstaviti datum ***šest mesecev*** pred datumom začetka veljavnosti].

Na Komisijo se prenese pooblastilo za dopolnitev te uredbe s sprejetjem regulativnih tehničnih standardov iz drugega pododstavka v skladu s členi 10 do 14 Uredbe (EU) št. 1093/2010, (EU) št. 1095/2010 oziroma (EU) št. 1094/2010.

Člen 24

Zahteve za preizkuševalce

1. Finančni subjekti ***in tretji ponudniki storitev IKT, ki smejo skleniti pogodbene dogovore neposredno z zunanjim preizkuševalcem v skladu s členom 23(2),*** za izvedbo penetracijskega testiranja na podlagi analize groženj uporabljajo samo preizkuševalce, ki:

   (a) so najprimernejši in uživajo največji ugled;

   (b) imajo tehnične in organizacijske zmogljivosti ter posebno strokovno znanje na področjih obveščevalnih podatkov o grožnjah, penetracijskega testiranja ali testiranja z rdečo ekipo;

   (c) so potrjeni s strani akreditacijskega organa v državi članici ali upoštevajo formalne kodekse ravnanja ali etične okvire***, ne glede na to, ali so iz Unije ali tretje države***;

   (d) ▌predložijo neodvisno zagotovilo ali revizijsko poročilo v zvezi z dobrim upravljanjem tveganj, povezanih z izvajanjem penetracijskega testiranja na podlagi analize groženj, vključno z ustrezno zaščito zaupnih informacij finančnega subjekta in povračilom škode za poslovna tveganja finančnega subjekta;

   (e) ▌imajo polno kritje z ustreznimi zavarovanji poklicne odgovornosti, vključno s kritjem za tveganje kršitve in malomarnosti***;***

   (ea) če gre za notranje preizkuševalce, testiranje opravljajo na podlagi odobritve ustreznega pristojnega organa in enotnega javnega organa, imenovanega v skladu s členom 23(3a), pri čemer ta organa preverita, ali ima finančni subjekt zadostna sredstva za ta namen, in ali je poskrbel, da se v fazah zasnove in izvedbe testiranja prepreči nasprotje interesov.

2. Finančni subjekti ***in tretji ponudniki storitev IKT, ki smejo skleniti pogodbene dogovore neposredno z zunanjim preizkuševalcem v skladu s členom 23(2),*** zagotovijo, da se v ***dogovorih***, sklenjenih z zunanjimi preizkuševalci, zahteva dobro upravljanje rezultatov penetracijskega testiranja na podlagi analize groženj in da kakršna koli obdelava rezultatov, vključno z ustvarjanjem, osnutki, shranjevanjem, združevanjem, poročanjem, obveščanjem ali uničenjem, finančnega subjekta ne izpostavlja tveganjem.

POGLAVJE V

UPRAVLJANJE TVEGANJ TRETJIH OSEB NA PODROČJU IKT

ODDELEK I

KLJUČNA NAČELA ZA DOBRO UPRAVLJANJE TVEGANJ TRETJIH OSEB NA PODROČJU IKT

Člen 25

Splošna načela

Finančni subjekti upravljajo tveganje tretjih oseb na področju IKT kot sestavni del tveganj na področju IKT v sklopu okvira za upravljanje tveganj na področju IKT v skladu z naslednjimi načeli:

1. Finančni subjekti, ki imajo za vodenje svojih poslovnih dejavnosti sklenjene pogodbene dogovore za uporabo storitev IKT, so ves čas v celoti odgovorni za izpolnjevanje in upoštevanje vseh obveznosti iz te uredbe in veljavne zakonodaje o finančnih storitvah.

2. Finančni subjekti upravljajo tveganja tretjih oseb na področju IKT glede na načelo sorazmernosti, pri čemer upoštevajo:

   (a) ***naravo,*** obseg, zapletenost in pomen odvisnosti, povezanih z IKT;

   (b) tveganja, ki izhajajo iz pogodbenih dogovorov o uporabi storitev IKT, sklenjenih s tretjimi ponudniki storitev IKT, ob upoštevanju kritičnosti ali pomena posamezne storitve, postopka ali funkcije ter možnega učinka na neprekinjenost in kakovost finančnih storitev in dejavnosti na individualni in skupinski ravni.

   (ba) ali je ponudnik storitev IKT ponudnik storitev IKT znotraj skupine.

3. Finančni subjekti***, ki niso mikropodjetja,*** kot del svojega okvira za upravljanje tveganj na področju IKT sprejmejo in redno pregledujejo strategijo o tveganju tretjih oseb na področju IKT ▌. Ta strategija vključuje politiko o uporabi storitev IKT, ki jih zagotavljajo tretji ponudniki storitev IKT, in se uporablja na posamični in, če je to ustrezno, na subkonsolidirani in konsolidirani ravni. Upravljalni organ redno pregleduje tveganja, ugotovljena v zvezi z oddajanjem kritičnih ali pomembnih funkcij v zunanje izvajanje.

4. Finančni subjekti v sklopu svojega okvira za upravljanje tveganj na področju IKT na ravni subjekta ter na subkonsolidirani in konsolidirani ravni vzdržujejo in posodabljajo register informacij v zvezi z vsemi pogodbenimi dogovori o uporabi storitev IKT***, ki podpirajo kritične ali pomembne funkcije***, ki jih zagotavljajo tretji ponudniki storitev IKT.

   Pogodbeni dogovori iz prvega pododstavka se ustrezno dokumentirajo ▌.

   Do začetka veljavnosti izvedbenih tehničnih standardov iz odstavka 10 finančni subjekti upoštevajo smernice in druge ukrepe, ki jih izdajo evropski nadzorni organi in pristojni organi, če so na voljo.

   Finančni subjekti pristojnim organom vsaj enkrat letno poročajo o številu novih dogovorov o uporabi storitev IKT***, ki podpirajo kritične ali pomembne funkcije***,

kategorijah tretjih ponudnikov storitev IKT, vrsti pogodbenih dogovorov ter storitvah in funkcijah, ki se zagotavljajo.

Finančni subjekti pristojnemu organu na zahtevo predložijo celoten register informacij ali, če se zahteva, določene oddelke registra, skupaj z vsemi informacijami, za katere se meni, da so potrebne za učinkovit nadzor finančnega subjekta.

Finančni subjekti pravočasno obvestijo pristojni organ o načrtovani sklenitvi pogodbe o uporabi kritičnih ali pomembnih funkcij in o tem, kdaj je funkcija postala kritična ali pomembna.

5. Finančni subjekti pred sklenitvijo pogodbenega dogovora o uporabi storitev IKT:

(a) ocenijo, ali pogodbeni dogovor zajema kritično ali pomembno funkcijo;

(b) ocenijo, ali so izpolnjeni nadzorni pogoji za sklenitev pogodbenega dogovora;

(c) opredelijo in ocenijo vsa pomembna tveganja v zvezi s pogodbenim dogovorom, vključno z možnostjo, da lahko taki pogodbeni dogovori prispevajo k povečanju tveganja koncentracije na področju IKT;

(d) opravijo skrben pregled potencialnih tretjih ponudnikov storitev IKT in s postopki izbire in ocenjevanja zagotovijo ustreznost tretjega ponudnika storitev IKT;

(e) opredelijo in ocenijo nasprotja interesov, ki jih lahko povzroči pogodbeni dogovor.

6. Finančni subjekti lahko sklepajo pogodbene dogovore samo s tretjimi ponudniki storitev IKT, ki izpolnjujejo visoke, ustrezne in ***posodobljene*** varnostne standarde. ***Pri ugotavljanju, ali so vzpostavljeni varnostni standardi ustrezni, se upoštevajo tudi najnovejši standardi.***

7. Finančni subjekti pri uveljavljanju pravic do dostopa, inšpekcijskih pregledov in revizij pri tretjem ponudniku storitev IKT ***v zvezi s kritičnimi in pomembnimi funkcijami*** vnaprej določijo pogostost revizij in inšpekcijskih pregledov ter področja, ki jih je treba revidirati, s pristopom, ki temelji na tveganju, in ob upoštevanju splošno sprejetih revizijskih standardov v skladu z vsemi nadzornimi navodili o uporabi in vključitvi takih revizijskih standardov.

Za pogodbene dogovore, ki vključujejo ***natančno opredeljeno tehnološko kompleksnost***, finančni subjekt preveri, ali imajo revizorji, ne glede na to, ali so to notranji revizorji, skupine revizorjev ali zunanji revizorji, ustrezne spretnosti in znanje za učinkovito izvajanje ustreznih revizij in ocen.

8. Finančni subjekti zagotovijo, da ▌ pogodbeni dogovori o uporabi storitev IKT finančnim subjektom ***omogočajo, da sprejmejo ustrezne popravljalne ali sanacijske ukrepe, ki bi lahko vključevali popolno odpoved dogovorov, če popravek ne bi bil mogoč, ali delno odpoved dogovorov, če bi bil v skladu z veljavno zakonodajo popravek mogoč***, vsaj v naslednjih okoliščinah:

(a) ***znatna*** kršitev veljavnih zakonov, predpisov ali pogodbenih pogojev s strani tretjega ponudnika storitev IKT;

(aa) priporočilo, ki ga je skupni nadzorni organ na podlagi člena 37 izdal ključnemu tretjemu ponudniku storitev IKT;

(b) okoliščine, ugotovljene med spremljanjem tveganja tretjih oseb na področju IKT, za katere se šteje, da lahko spremenijo izvajanje funkcij, zagotovljenih s pogodbenim dogovorom, vključno s pomembnimi spremembami, ki vplivajo na dogovor ali položaj tretjega ponudnika storitev IKT;

(c) dokazane pomanjkljivosti tretjega ponudnika storitev IKT ***v zvezi s*** splošnim upravljanjem tveganj na področju IKT ***pri njegovi pogodbi s finančnim subjektom*** in zlasti v načinu, kako zagotavlja varnost in celovitost zaupnih, osebnih ali kako drugače občutljivih podatkov ali neosebnih informacij;

(d) okoliščine, ko pristojni organ zaradi zadevnega pogodbenega dogovora ***dokazano*** ne more več učinkovito nadzirati finančnega subjekta.

8a. Da bi se zmanjšalo tveganje motenj na ravni finančnega subjekta, se lahko finančni subjekt v ustrezno utemeljenih okoliščinah in v dogovoru s svojimi pristojnimi organi odloči, da ne bo odpovedal pogodbenih dogovorov s tretjim ponudnikom storitev IKT, dokler ga ne more zamenjati ali preiti na notranje rešitve, ki bodo ustrezne glede na kompleksnost zagotovljene storitve, v skladu z izhodno strategijo iz odstavka 9.

8b. V primerih, ko se pogodbeni dogovori s tretjimi ponudniki storitev IKT odpovejo zaradi katere od okoliščin iz točk (a) do (d) odstavka 8, finančni subjekti ne krijejo stroškov prenosa podatkov od tretjega ponudnika storitev IKT, kadar presegajo stroške prenosa podatkov, določene v prvotni pogodbi.

9. ***Za storitve IKT, povezane s kritičnimi ali pomembnimi funkcijami,*** finančni subjekti vzpostavijo izhodne strategije***, ki se redno pregledujejo***. ***Izhodne strategije*** upoštevajo tveganja, ki se lahko pojavijo na ravni tretjega ponudnika storitev IKT, zlasti njegovo morebitno prenehanje delovanja, poslabšanje kakovosti zagotovljenih funkcij, kakršne koli motnje v poslovanju zaradi neprimernega ali neuspešnega opravljanja storitev ali pomembno tveganje, ki izhaja iz ustrezne in stalne uporabe funkcije***, ali v primeru odpovedi pogodbenih dogovorov s tretjimi ponudniki storitev IKT v koli od okoliščin iz točk (a) do (d) odstavka 8***.

Finančni subjekti zagotovijo, da lahko prekinejo pogodbene dogovore brez:

(a) motenj svojih poslovnih dejavnostih;

(b) omejevanja skladnosti z zakonskimi zahtevami;

(c) škode za neprekinjenost in kakovost zagotavljanja storitev strankam.

Načrti za prekinitev pogodbe morajo biti izčrpni, dokumentirani in po potrebi zadostno preizkušeni.

Finančni subjekti opredelijo alternativne rešitve in oblikujejo prehodne načrte, ki jim omogočajo, da tretjemu ponudniku storitev IKT odvzamejo pogodbene funkcije in ustrezne podatke ter jih varno in celovito prenesejo k alternativnim ponudnikom ali jih ponovno vključijo v lastno podjetje.

Finančni subjekti v vseh okoliščinah iz prvega pododstavka sprejmejo ustrezne ukrepe ob nepredvidljivih dogodkih za ohranjanje neprekinjenosti poslovanja.

10. Evropski nadzorni organi prek Skupnega odbora pripravijo osnutke izvedbenih tehničnih standardov za vzpostavitev standardnih predlog za namene registra informacij iz odstavka 4.

Te osnutke izvedbenih tehničnih standardov predložijo Komisiji do [UL: vstaviti datum

eno leto po datumu začetka veljavnosti te uredbe].

Na Komisijo se prenese pooblastilo za sprejetje izvedbenih tehničnih standardov iz prvega pododstavka v skladu s členom 15 Uredbe (EU) št. 1093/2010, (EU) št. 1095/2010 oziroma (EU) št. 1094/2010.

11. Evropski nadzorni organi prek Skupnega odbora pripravijo osnutke regulativnih standardov, da:

(a) nadalje opredelijo podrobno vsebino politike iz odstavka 3 v zvezi s pogodbenimi dogovori o uporabi storitev IKT, ki jih zagotavljajo tretji ponudniki storitev IKT, s sklicevanjem na glavne faze življenjskega cikla zadevnih dogovorov o uporabi storitev IKT;

(b) nadalje opredelijo vrste informacij, ki jih je treba vključiti v register informacij iz odstavka 4.

Evropski nadzorni organi te osnutke regulativnih tehničnih standardov Komisiji predložijo do [UP: vstaviti datum ***18 mesecev*** po datumu začetka veljavnosti te uredbe].

Na Komisijo se prenese pooblastilo za dopolnitev te uredbe s sprejetjem regulativnih tehničnih standardov iz drugega pododstavka v skladu s členi 10 do 14 Uredbe (EU) št. 1093/2010, (EU) št. 1095/2010 oziroma (EU) št. 1094/2010.

Člen 26

Predhodna ocena tveganja koncentracije na področju IKT in dogovorov o nadaljnjem zunanjem podizvajanju

1. Finančni subjekti pri ugotavljanju in ocenjevanju tveganja koncentracije na področju IKT iz točke (c) člena 25(5) upoštevajo, ali bi sklenitev pogodbenega dogovora v zvezi s storitvami IKT***, ki podpirajo kritične ali pomembne funkcije***, povzročila:

(a) sklenitev pogodbe s tretjim ponudnikom storitev IKT, ki ga ni enostavno nadomestiti, ali

(b) obstoj več pogodbenih dogovorov v zvezi z zagotavljanjem storitev IKT***, ki podpirajo kritične ali pomembne funkcije,*** z istim tretjim ponudnikom storitev IKT ali tesno povezanimi tretjimi ponudniki storitev IKT.

Finančni subjekti pretehtajo koristi in stroške alternativnih rešitev, kot je uporaba različnih tretjih ponudnikov storitev IKT, pri čemer upoštevajo, ali in kako predvidene rešitve ustrezajo poslovnim potrebam in ciljem iz njihove strategije za digitalno odpornost.

2. Kadar pogodbeni dogovor o uporabi storitev IKT***, ki podpirajo kritične ali pomembne funkcije,*** vključuje možnost, da tretji ponudnik storitev IKT kritično ali pomembno funkcijo nadalje odda v podizvajanje drugim tretjim ponudnikom storitev IKT, finančni subjekti pretehtajo koristi in tveganja, ki lahko nastanejo v povezavi s tako morebitno oddajo v podizvajanje ▌.

Kadar se pogodbeni dogovori o uporabi storitev IKT***, ki podpirajo kritične ali pomembne funkcije***, sklenejo s tretjim ponudnikom storitev IKT ▌, finančni subjekti za pomembne štejejo vsaj naslednje dejavnike:

(a) ▌

(b) ▌

(c) določbe insolvenčnega prava, ki bi veljale v primeru stečaja tretjega ponudnika storitev IKT, ***ter***

(d) vse omejitve, ki se lahko pojavijo v zvezi z nujno obnovitvijo podatkov finančnega subjekta.

Kadar se pogodbeni dogovori o uporabi storitev IKT, ki podpirajo kritične ali pomembne funkcije, sklenejo s tretjim ponudnikom storitev IKT s sedežem v tretji državi, finančni subjekti poleg dejavnikov iz prvega in drugega pododstavka upoštevajo še:

(i) spoštovanje varstva podatkov Unije in

(ii) učinkovito izvrševanje pravil iz te uredbe.

Kadar ti pogodbeni dogovori vključujejo podizvajanje kritičnih ali pomembnih funkcij, finančni subjekti ocenijo, ali in kako lahko potencialno dolge ali zapletene verige podizvajanja vplivajo na njihovo zmožnost***, da v celoti ocenijo dejavnike iz drugega in tretjega pododstavka za spremljanje pogodbenih funkcij***, ter zmožnost pristojnega organa, da v zvezi s tem učinkovito nadzoruje finančni subjekt.

Člen 27

Ključne pogodbene določbe

1. Pravice in obveznosti finančnega subjekta in tretjega ponudnika storitev IKT se jasno dodelijo in določijo v pisni obliki. Celotna pogodba, ki vključuje sporazume o ravni storitev, se dokumentira ***v pisni obliki in da*** na voljo strankam v papirni obliki ali obliki, ki jo je mogoče prenesti in do nje dostopati.

2. ***Finančni subjekti in tretji ponudniki storitev IKT zagotovijo, da*** pogodbeni dogovori o uporabi storitev IKT vključujejo vsaj naslednje:

(a) jasen in popoln opis vseh funkcij in storitev, ki jih mora zagotoviti tretji ponudnik storitev IKT, z navedbo, ali je dovoljeno oddajanje kritične ali pomembne funkcije ali njenih bistvenih delov v podizvajanje in, če je dovoljeno, pogoje, ki veljajo za tako podizvajanje;

(b) lokacije **–** ***regije ali države*** **–**, kjer se bodo zagotavljale pogodbene funkcije in storitve ***IKT***, oddane v izvajanje ali podizvajanje, in obdelovali podatki, vključno z lokacijo hrambe, ter zahtevo, da tretji ponudnik storitev IKT ***vnaprej*** obvesti finančnega subjekta, če namerava spremeniti te lokacije;

(c) določbe o dostopnosti, razpoložljivosti, celovitosti, varnosti, ***zaupnosti*** in zaščiti ▌ podatkov***, vključno z osebnimi podatki***;

(ca) določbe o zagotavljanju dostopa, obnovitve in vrnitve v preprosto dostopni obliki osebnih in neosebnih podatkov, ki jih obdeluje finančni subjekt, v primeru insolventnosti, reševanja ali prenehanja poslovanja tretjega ponudnika storitev IKT ***ali v primeru odpovedi pogodbenih dogovorov***;

(d) celovite opise ravni storitev, vključno z njihovimi posodobitvami in popravki, ter natančne kvantitativne in kvalitativne cilje uspešnosti znotraj dogovorjenih ravni storitev, da lahko finančni subjekt učinkovito spremlja in brez nepotrebnega odlašanja omogoči ustrezne popravne ukrepe, kadar dogovorjene

ravni storitev niso dosežene;

(e) ▌

(f) obveznost tretjega ponudnika storitev IKT, da v primeru incidenta ***v zvezi z zagotavljano storitvijo***, povezanega z IKT, zagotavlja pomoč brez dodatnih stroškov ali po predhodno določeni ceni;

(g) zahteve, da tretji ponudnik storitev IKT izvaja in testira poslovne načrte izrednih ukrepov ter vzpostavi varnostne ukrepe, orodja in politike na področju IKT, ki finančnemu subjektu ▌zagotavljajo opravljanje storitev ***z ustrezno ravnjo varnosti*** v skladu z njegovim regulativnim okvirom;

(h) ▌

(i) obveznost tretjega ponudnika storitev IKT, da v celoti sodeluje s pristojnimi organi in organi za reševanje finančnega subjekta, vključno z osebami, ki jih ti imenujejo;

(j) pravice do odpovedi in s tem povezane minimalne roke za odpoved pogodbe v skladu s pričakovanji pristojnih organov ***in organov za reševanje ter, kadar ta pogodbeni dogovor vpliva na ponudnika storitev znotraj skupine IKT, ki je ponudnik znotraj iste skupine, analizo na podlagi pristopa, ki temelji na tveganju***;

(k) izhodne strategije, zlasti določitev obveznega ustreznega prehodnega obdobja:

(i) med katerim bo tretji ponudnik storitev IKT še naprej zagotavljal ustrezne funkcije ali storitve, da bi zmanjšal tveganje motenj pri finančnem subjektu ***ali zagotovil učinkovito rešitev in prestrukturiranje***;

(ii) ki finančnemu subjektu omogoča, da preide na drugega tretjega ponudnika storitev IKT ali na rešitve na mestu uporabe, ki so skladne z zapletenostjo zagotovljene storitve.

(iia) kadar ta pogodbeni dogovor vpliva na ponudnika storitev IKT znotraj skupine, ki je ponudnik znotraj iste skupine, se analizira na podlagi pristopa, ki temelji na tveganju;

(ka) določbo o obdelavi osebnih podatkov s strani tretjega ponudnika storitev IKT, ki mora biti skladna z Uredbo (EU) 2016/679;

2a. Pogodbeni dogovori za zagotavljanje kritičnih ali pomembnih funkcij poleg odstavka 2 vključujejo vsaj naslednje:

(a) odpovedne roke in obveznosti tretjega ponudnika storitev IKT za poročanje finančnemu subjektu, vključno z obveščanjem o spremembah, ki bi lahko pomembno vplivale na zmožnost tretjega ponudnika storitev IKT, da učinkovito izvaja kritične ali pomembne funkcije v skladu z dogovorjenimi ravnmi storitev;

(b) pravico do stalnega spremljanja uspešnosti tretjega ponudnika storitev IKT, ki vključuje:

(i) pravice do dostopa, inšpekcijskega pregleda in revizije s strani finančnega subjekta ali imenovane tretje osebe ter pravico do pregleda

kopij ustrezne dokumentacije na kraju samem, če je kritična za poslovanje tretjih ponudnikov storitev IKT, pri čemer drugi pogodbeni dogovori ali izvedbene politike ne ovirajo ali omejujejo učinkovitega uveljavljanja teh pravic;

(ii) pravico, da se zahtevajo alternativne ravni zanesljivosti, če so prizadete pravice drugih strank;

(iii) zavezo tretjega ponudnika storitev IKT, da bo v celoti sodeloval pri inšpekcijskih pregledih in revizijah na kraju samem, ki jih izvajajo pristojni organi, glavni nadzornik, finančni subjekt ali imenovana tretja oseba, ter podrobnosti o obsegu, načinih in pogostosti teh inšpekcijskih pregledov in revizij;

Z odstopanjem od točke (b) se lahko tretji ponudnik storitev IKT in finančni subjekt dogovorita, da se lahko pravice do dostopa, inšpekcijskega pregleda in revizije prenesejo na neodvisno tretjo stran, ki jo imenuje tretji ponudnik storitev IKT, finančni subjekt pa lahko od tretje strani kadarkoli zahteva informacije in zagotovila glede uspešnosti tretjega ponudnika storitev IKT.

2b. Za pogodbene dogovore v zvezi z zagotavljanjem storitev IKT s tretjim ponudnikom storitev IKT s sedežem v tretji državi, imenovanim za ključnega v skladu s členom 28(9), poleg določb iz odstavkov 2 in 2a tega člena velja naslednje:

(a) določajo, da pogodbo ureja zakonodaja države članice, ter

(b) zagotavljajo, da lahko skupni nadzorni organ in glavni nadzornik opravljata svoje naloge iz člena 30 na podlagi svojih pristojnosti iz člena 31.

Ni treba, da storitve, za katere so sklenjeni pogodbeni dogovori, opravljajo podjetja, ustanovljena v Uniji v skladu z zakonodajo države članice.

3. Pri pogajanjih o pogodbenih dogovorih finančni subjekti in tretji ponudniki storitev IKT upoštevajo uporabo standardnih pogodbenih klavzul, pripravljenih za določene storitve.

3a. Pristojni organi imajo dostop do pogodbenih dogovorov iz tega člena. Stranke teh pogodbenih dogovorov se lahko dogovorijo za redigiranje poslovno občutljivih ali zaupnih informacij, preden pristojnim organom odobrijo dostop, pod pogojem, da jih v celoti obvestijo o obsegu in naravi redigiranja.

4. Evropski nadzorni organi prek Skupnega odbora pripravijo osnutke regulativnih tehničnih standardov, da natančneje opredelijo elemente, ki jih mora finančni subjekt določiti in oceniti pri oddaji kritičnih ali pomembnih funkcij v podizvajanje, da se pravilno izvršijo določbe točke (a) odstavka 2. ***Evropski nadzorni organi pri pripravi teh osnutkov regulativnih tehničnih standardov upoštevajo velikost finančnih subjektov, naravo, obseg in kompleksnost njihovih storitev, dejavnosti in poslovanja ter njihov splošni profil tveganja.***

Evropski nadzorni organi te osnutke regulativnih tehničnih standardov Komisiji predložijo do [UP: vstaviti datum ***18 mesecev*** po datumu začetka veljavnosti te uredbe].

Na Komisijo se prenese pooblastilo za dopolnitev te uredbe s sprejetjem regulativnih tehničnih standardov iz prvega pododstavka v skladu s členi 10 do 14 Uredbe (EU) št. 1093/2010, (EU) št. 1095/2010 oziroma (EU) št. 1094/2010.

ODDELEK II

OKVIR NADZORA KLJUČNIH TRETJIH PONUDNIKOV STORITEV IKT

Člen 28

Imenovanje ključnih tretjih ponudnikov storitev IKT

1. Evropski nadzorni organi prek Skupnega odbora in na podlagi priporočila nadzorniškega ***organa***, ustanovljenega v skladu s členom 29(1) ***po posvetovanju z ENISA***:

   (a) imenujejo tretje ponudnike storitev IKT, ki so ključni za finančne subjekte, ob upoštevanju meril iz odstavka 2;

   (b) imenujejo EBA, ESMA ali EIOPA za glavnega nadzornika za vsakega ključnega tretjega ponudnika storitev IKT, odvisno od tega, ali skupna vrednost sredstev finančnih subjektov, ki uporabljajo storitve navedenega ključnega tretjega ponudnika storitev IKT in ki jih zajema ena od uredb (EU) št. 1093/2010 (EU), št. 1094/2010 oziroma (EU) št. 1095/2010, predstavlja več kot polovico vrednosti celotnih sredstev vseh finančnih subjektov, ki uporabljajo storitve ključnega tretjega ponudnika storitev IKT, kar dokazujejo konsolidirane bilance stanja ali, kadar bilance stanja niso konsolidirane, posamezne bilance stanja navedenih finančnih subjektov.

   Glavni nadzornik, imenovan v skladu s točko (b) prvega pododstavka, je odgovoren za vsakodnevni nadzor ključnega tretjega ponudnika storitev IKT.

2. Imenovanje iz točke (a) odstavka 1 temelji na vseh naslednjih merilih:

   (a) sistemski učinek na stabilnost, neprekinjenost ali kakovost opravljanja finančnih storitev, če bi se zadevni tretji ponudnik storitev IKT soočal z veliko motnjo v delovanju pri zagotavljanju svojih storitev, ob upoštevanju števila finančnih subjektov, ki jim zadevni tretji ponudnik storitev IKT zagotavlja storitve;

   (b) sistemski značaj ali pomen finančnih subjektov, ki so odvisni od zadevnega tretjega ponudnika storitev IKT, ocenjen v skladu z naslednjimi parametri:

      i) število globalnih sistemsko pomembnih institucij (GSPI) ali drugih sistemsko pomembnih institucij (DSPI), ki so odvisne od zadevnega tretjega ponudnika storitev IKT;

      ii) soodvisnost med GSPI ali DSPI iz točke (i) in drugimi finančnimi subjekti, vključno s situacijami, ko GSPI ali DSPI drugim finančnim subjektom zagotavljajo storitve finančne infrastrukture;

   (c) odvisnost finančnih subjektov od storitev, ki jih zagotavlja zadevni tretji ponudnik storitev IKT v zvezi s kritičnimi ali pomembnimi funkcijami finančnih subjektov, ki nazadnje vključujejo istega tretjega ponudnika storitev IKT, ne glede na to, ali so finančni subjekti od teh storitev odvisni neposredno ali posredno, s sredstvi ali dogovori o podizvajanju;

   (d) stopnja nadomestljivosti tretjega ponudnika storitev IKT, ob upoštevanju naslednjih parametrov:

      i) pomanjkanje resničnih alternativ, celo delnih, zaradi omejenega števila tretjih ponudnikov storitev IKT, ki delujejo na določenem trgu, ali tržnega

deleža zadevnega tretjega ponudnika storitev IKT ali zaradi obstoječe tehnične zapletenosti ali izpopolnjenosti, tudi v zvezi s kakršno koli zaščiteno tehnologijo ali posebnostmi organizacije ali dejavnosti tretjega ponudnika storitev IKT;

ii) težave pri delni ali popolni selitvi ustreznih podatkov in delovnih obremenitev z zadevnega na drugega tretjega ponudnika storitev IKT, bodisi zaradi znatnih finančnih stroškov, časa ali druge vrste virov, ki jih lahko povzroči postopek selitve, bodisi zaradi povečanih tveganj na področju IKT ali drugih operativnih tveganj, ki jim je finančni subjekt lahko izpostavljen s tako selitvijo;

(e) število držav članic, v katerih zadevni tretji ponudnik storitev IKT zagotavlja storitve;

(f) število držav članic, v katerih delujejo finančni subjekti, ki uporabljajo zadevnega tretjega ponudnika storitev IKT.

(fa) pomen in bistvenost storitev, ki jih zagotavlja zadevni tretji ponudnik storitev IKT.

2a. Skupni nadzorni organ obvesti tretjega ponudnika storitev IKT, preden začne oceno za namene imenovanja iz točke (a) odstavka 1.

Skupni nadzorni organ obvesti tretjega ponudnika storitev IKT o rezultatu ocene iz prvega pododstavka tako, da mu predloži osnutek priporočila o kritičnosti. Tretji ponudnik storitev IKT lahko v šestih tednih od datuma prejema osnutka priporočila skupnemu nadzornemu organu predloži utemeljeno izjavo o oceni. Ta vsebuje vse relevantne dodatne informacije, za katere tretji ponudnik storitev IKT meni, da so primerne za potrditev popolnosti in točnosti postopka imenovanja ali za izpodbijanje osnutka priporočila o kritičnosti. Skupni odbor evropskih nadzornih organov pripombe ustrezno upošteva in lahko od tretjega ponudnika storitev IKT zahteva dodatne informacije ali dokaze, preden sprejme odločitev o imenovanju.

Skupni odbor evropskih nadzornih organov obvesti tretjega ponudnika storitev IKT, da je bil imenovan za ključnega. Tretji ponudnik storitev IKT ima vsaj tri mesece od datuma prejema obvestila, da opravi potrebne prilagoditve, ki bi skupnemu nadzornemu organu omogočile izvajanje njegovih dolžnosti v skladu s členom 30, ter da obvesti finančne subjekte, ki jim tretji ponudnik storitev IKT zagotavlja storitve. Skupni nadzorni organ lahko dovoli, da se prilagoditveno obdobje podaljša za največ tri mesece, če to zahteva in ustrezno utemelji imenovani tretji ponudnik storitev IKT.

3. Komisiji se v skladu s členom 50 podeli pooblastilo za sprejetje delegiranih aktov za ***natančnejšo opredelitev*** meril iz odstavka 2.

4. Mehanizem imenovanja iz točke (a) odstavka 1 se ne uporablja, dokler Komisija ne sprejme delegiranega akta v skladu z odstavkom 3.

5. Mehanizem imenovanja iz točke (a) odstavka 1 se ne uporablja v zvezi s tretjimi ponudniki storitev IKT, za katere veljajo okviri nadzora, vzpostavljeni za podpiranje nalog iz člena 127(2) Pogodbe o delovanju Evropske unije.

6. ***Skupni nadzorni organ v posvetovanju z ENISA*** prek Skupnega odbora pripravi, objavi in ***redno*** posodobi seznam ključnih tretjih ponudnikov storitev IKT na ravni Unije.

7. Za namene točke (a) odstavka 1 pristojni organi na letni in zbirni ravni pošljejo poročila iz člena 25(4) ***skupnemu nadzornemu organu***, ustanovljenemu v skladu s členom 29. ***Skupni nadzorni organ*** na podlagi informacij, ki jih prejme od pristojnih organov, oceni odvisnosti finančnih subjektov od tretjih oseb na področju IKT.

8. Tretji ponudniki storitev IKT, ki niso vključeni na seznam iz odstavka 6, lahko zaprosijo za vključitev na navedeni seznam.

Za namene prvega pododstavka tretji ponudnik storitev IKT predloži utemeljeno zahtevo EBA, ESMA ali EIOPA, ki se prek Skupnega odbora odloči, ali bo navedenega tretjega ponudnika storitev IKT vključila na navedeni seznam v skladu s točko (a) odstavka 1.

Odločitev iz drugega pododstavka se sprejme in sporoči tretjemu ponudniku storitev IKT v šestih mesecih po prejemu vloge.

8a. Skupni odbor evropskih nadzornih organov na priporočilo skupnega nadzornega organa imenuje tretje ponudnike storitev IKT s sedežem v tretji državi, ki so ključni za finančne subjekte, v skladu s točko (a) odstavka 1.

Evropski nadzorni organi in skupni nadzorni organ pri imenovanju iz prvega pododstavka tega odstavka upoštevajo postopkovne korake iz odstavka 2a.

9. Finančni subjekti ne smejo uporabljati ***ključnega*** tretjega ponudnika storitev IKT s sedežem v tretji državi***, razen če ima ta tretji ponudnik storitev IKT podjetje, ustanovljeno v Uniji v skladu z zakonodajo države članice, in je sklenil pogodbene dogovore v skladu s členom 27(2b)***.

Člen 29

Struktura nadzornega okvira

1. Skupni ***nadzorni organ se ustanovi*** za namene ***izvajanja nadzora*** tveganj tretjih oseb na področju IKT v finančnih sektorjih ***in za opravljanje neposrednega nadzora tretjih ponudnikov storitev IKT, ki so imenovani za ključne v skladu s členom 28***.

Vloga skupnega nadzornega organa je omejena na nadzorna pooblastila v zvezi s tveganji na področju IKT, povezanimi s storitvami IKT, ki jih za finančne subjekte zagotavljajo ključni tretji ponudniki storitev IKT.

Skupni nadzorni organ redno razpravlja o pomembnih spremembah pri tveganjih in ranljivostih na področju IKT ter spodbuja dosleden pristop pri spremljanju tveganj tretjih oseb na področju IKT na ravni Unije.

2. ***Skupni nadzorni organ*** enkrat letno opravi kolektivno oceno rezultatov in ugotovitev nadzornih dejavnosti, ki se izvajajo za vse ključne tretje ponudnike storitev IKT, in spodbuja usklajevalne ukrepe za povečanje digitalne operativne odpornosti finančnih subjektov ter spodbujanje dobrih praks pri obravnavanju tveganj koncentracije na področju IKT in raziskovanje načinov za zmanjševanje tveganja za medsektorske prenose tveganja.

Skupni nadzorni organ predloži izčrpne referenčne vrednosti ključnih tretjih ponudnikov storitev IKT, ki jih Skupni odbor sprejme kot skupna stališča evropskih nadzornih organov v skladu s členom 56(1) uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010.

3. ***Skupni nadzorni organ*** je sestavljen iz ***izvršnih direktorjev*** evropskih nadzornih

organov***,*** enega predstavnika na visoki ravni, ki je izbran iz osebja evropskih nadzornih organov***, ter enega predstavnika na visoki ravni iz vsaj osmih pristojnih nacionalnih organov***. Po en predstavnik Evropske komisije, ESRB, ECB in ENISA ***ter vsaj en neodvisni strokovnjak, ki je izbran v skladu s členom 3a tega člena,*** sodelujejo ▌ kot opazovalci.

Skupni odbor evropskih nadzornih organov po letnem imenovanju ključnih tretjih ponudnikov storitev IKT v skladu s členom 28(1) odloči, kateri pristojni nacionalni organi naj bodo člani skupnega nadzornega organa, pri tem pa upošteva naslednje dejavnike:

(a) število ključnih tretjih ponudnikov storitev IKT, ki imajo sedež ali zagotavljajo storitve v državi članici;

(b) zanašanje finančnih subjektov v državi članici na ključne tretje ponudnike storitev IKT;

(c) sorazmerno strokovnost pristojnega nacionalnega organa;

(d) razpoložljivost sredstev in zmogljivosti pristojnega nacionalnega organa;

(e) potrebo po racionalizaciji, varčnosti in učinkovitosti delovanja in odločanja skupnega nadzornega organa.

Skupni nadzorni organ svojo dokumentacijo in odločitve posreduje vsem pristojnim nacionalnim organom, ki niso člani skupnega nadzornega organa.

Skupni nadzorni organ dela ob podpori in pomoči namenskega osebja iz vseh evropskih nadzornih organov.

3a. Skupni nadzorni organ imenuje neodvisnega strokovnjaka iz odstavka 3 tega člena kot opazovalca na podlagi javnega in preglednega postopka prijave.

Neodvisni strokovnjak je imenovan za obdobje dveh let na podlagi strokovnega znanja o finančni stabilnosti, digitalni operativni odpornosti in varnostnih vprašanjih, povezanih z IKT.

Imenovani neodvisni strokovnjak nima druge funkcije na nacionalni ali mednarodni ravni ali na ravni Unije. Neodvisni strokovnjak deluje neodvisno in objektivno, izključno v interesu Unije kot celote ter ne zahteva in ne sprejema navodil institucij ali organov Unije, katere koli vlade države članice ali katerih koli drugih javnih ali zasebnih organov.

Skupni nadzorni organ se lahko odloči, da imenuje več kot enega neodvisnega strokovnega opazovalca.

4. Evropski nadzorni organi v skladu s členom 16 uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010 ***do [UL: vstaviti datum 18 mesecev po začetku veljavnosti te uredbe]*** izdajo smernice o sodelovanju med ***skupnim nadzornim organom, glavnim nadzornikom*** in pristojnimi organi za namene tega oddelka v zvezi s podrobnimi postopki in pogoji glede izvajanja nalog med pristojnimi organi in ***skupnim nadzornim organom*** ter glede podrobnosti o izmenjavi informacij, ki jih pristojni organi potrebujejo za zagotovitev nadaljnjega ukrepanja na podlagi priporočil, ki jih ***skupni nadzorni organ*** naslovi na ključne tretje ponudnike storitev IKT v skladu s točko (d) člena 31(1).

5. Zahteve iz tega oddelka ne posegajo v uporabo Direktive (EU) 2016/1148 in drugih

pravil Unije o nadzoru, ki veljajo za ponudnike storitev računalništva v oblaku.

6. Skupni nadzorni ***organ*** enkrat letno Evropskemu parlamentu, Svetu in Komisiji predloži poročilo o uporabi tega oddelka.

Člen 30

Naloge glavnega nadzornika

1. Glavni nadzornik***, imenovan v skladu s točko (b) člena 28(1), vodi in usklajuje vsakodnevni nadzor ključnih tretjih ponudnikov storitev IKT ter je glavna kontaktna točka zanje.***

1a. ***Glavni nadzornik*** oceni, ali ima vsak ključni tretji ponudnik storitev IKT vzpostavljena celovita, zanesljiva in učinkovita pravila, postopke, mehanizme in dogovore za upravljanje tveganj na področju IKT, ki jih lahko kot tak predstavlja za finančne subjekte. ***Pri oceni se osredotoča predvsem na storitve IKT, ki podpirajo kritične ali pomembne funkcije, ki jih ključni tretji ponudnik storitev IKT zagotavlja finančnim subjektom, lahko pa je tudi širša, če je pomembna za oceno tveganj teh funkcij.***

2. Ocena iz odstavka 1***a*** vključuje:

   (a) zahteve v zvezi IKT, da se zagotovijo zlasti varnost, razpoložljivost, neprekinjenost, nadgradljivost in kakovost storitev, ki jih ključni tretji ponudnik storitev IKT zagotavlja finančnim subjektom, ter zmožnost stalnega ohranjanja visokih standardov glede varnosti, zaupnosti in celovitosti podatkov;

   (b) fizično varnost, ki prispeva k zagotavljanju varnosti IKT, vključno z varnostjo prostorov, objektov in podatkovnih centrov;

   (c) postopke upravljanja tveganj, vključno s politikami upravljanja tveganj na področju IKT, neprekinjenim poslovanjem na področju IKT in načrti okrevanja IKT po katastrofi;

   (d) ureditve upravljanja, vključno z organizacijsko strukturo z jasnimi, preglednimi in doslednimi opredelitvami pristojnosti in odgovornosti, ki omogočajo učinkovito upravljanje tveganj IKT;

   (e) opredelitev in spremljanje ***večjih*** incidentov, povezanih z IKT, takojšnje poročanje finančnim subjektom o njih ter upravljanje in reševanje teh incidentov, zlasti kibernetskih napadov;

   (f) mehanizme za prenosljivost podatkov, prenosljivost aplikacij in interoperabilnost, ki finančnim subjektom zagotavljajo učinkovito uveljavljanje pravic do odpovedi;

   (g) testiranje sistemov, infrastrukture in kontrol IKT;

   (h) revizije IKT;

   (i) uporabo ustreznih nacionalnih in mednarodnih standardov, ki se uporabljajo za zagotavljanje ponudnikovih storitev IKT finančnim subjektom.

3. ***Skupni nadzorni organ*** na podlagi ocene iz odstavka ***1a, ki jo opravi glavni nadzornik, pripravi in predlaga*** jasen, podroben in obrazložen individualni načrt nadzora za vsakega ključnega tretjega ponudnika storitev IKT***, kar pa koordinira in vodi glavni nadzornik***.

Skupni nadzorni organ se pri pripravi osnutka načrta nadzora posvetuje z vsemi ustreznimi pristojnimi organi in enotnimi kontaktnimi točkami iz člena 8 Direktive (EU) 2016/1148, da se prepreči vsakršna neskladnost ali podvajanje z obveznostmi ključnega tretjega ponudnika storitev IKT iz navedene direktive.

Načrt nadzora vsako leto sprejme upravni odbor glavnega nadzornika.

Osnutek načrta nadzora se vsako leto posreduje ključnemu tretjemu ponudniku storitev IKT.

Po prejemu osnutka načrta nadzora ima ključni tretji ponudnik storitev IKT na voljo šest tednov, da ga pregleda in predloži obrazloženo izjavo o njem. Ključni tretji ponudnik storitev IKT lahko tako obrazloženo izjavo predloži le, če lahko predloži dokaze, da bi izvajanje načrta nadzora nesorazmerno vplivalo na stranke, za katere se ta uredba ne uporablja, ali jim povzročilo motnje, oziroma da obstaja uspešnejša ali učinkovitejša rešitev za obvladovanje ugotovljenih tveganj na področju IKT. Če tako izjavo predloži, ključni tretji ponudnik storitev IKT skupnemu nadzornemu organu predlaga uspešnejšo ali učinkovitejšo rešitev za doseganje ciljev osnutka načrta nadzora.

Odbor glavnega nadzornika obrazloženo izjavo ustrezno upošteva in lahko od tretjega ponudnika storitev IKT zahteva dodatne informacije ali dokaze.

4. Ko so letni načrti nadzora iz odstavka 3 ***sprejeti*** in posredovani ključnih tretjim ponudnikom storitev IKT, lahko pristojni organi sprejmejo ukrepe v zvezi s ključnimi tretjimi ponudniki storitev IKT samo v dogovoru ***s skupnim nadzornim organom***.

Člen 31

Nadzorna pooblastila

1. Za namene izvajanja nalog, določenih v tem oddelku, ima glavni nadzornik naslednja pooblastila ***v povezavi s storitvami, ki jih finančnim subjektom zagotavljajo ključni tretji ponudniki storitev IKT***:

   (a) da zahteva vse ustrezne informacije in dokumentacijo v skladu s členom 32;

   (b) da izvaja splošne preiskave in inšpekcijske preglede ***na kraju samem*** v skladu s členoma 33 in 34;

   (c) da zahteva poročila po zaključku nadzornih dejavnosti, v katerih so navedeni sprejeti ukrepi ali popravni ukrepi, ki so jih izvedli ključni tretji ponudniki storitev IKT v zvezi s priporočili iz ▌ odstavka ***1a***;

1a. Za izvajanje nalog, določenih v tem oddelku, ter na podlagi informacij, ki jih je pridobil glavni nadzornik, in rezultatov preiskav, ki jih je opravil glavni nadzornik, je skupni nadzorni organ pristojen, da obravnava priporočila na področjih iz člena 30(2), zlasti glede:

   (i) uporabe posebnih zahtev ali postopkov glede kakovosti in varnosti IKT, zlasti v zvezi z uvedbo popravkov, posodobitev, šifriranja in drugih varnostnih ukrepov, za katere ***skupni nadzorni organ*** meni, da so pomembni za zagotavljanje varnosti storitev na področju IKT, ki se zagotavljajo finančnim subjektom;

   (ii) uporabe pogojev, vključno z njihovo tehnično izvedbo, pod katerimi ključni tretji ponudniki storitev IKT zagotavljajo storitve finančnim subjektom in za katere ***skupni nadzorni organ*** meni, da so pomembni za preprečevanje nastanka

ali povečanja kritičnih točk odpovedi ali za zmanjšanje možnih sistemskih učinkov na finančni sektor Unije v primeru tveganja koncentracije na področju IKT;

(iii) vsake načrtovane oddaje v podizvajanje, vključno z zunanjim podizvajanjem, kadar po pregledu dogovorov o podizvajanju, opravljenem v skladu s členoma 32 in 33, vključno z dogovori o zunanjem podizvajanju, ki jih ključni tretji ponudniki storitev IKT nameravajo skleniti z drugimi tretjimi ponudniki storitev IKT ali podizvajalci storitev IKT s sedežem v tretji državi, ***skupni nadzorni organ*** meni, da lahko nadaljnje podizvajanje povzroči tveganja za zagotavljanje storitev s strani finančnega subjekta ali tveganja za finančno stabilnost;

(iv) opustitve sklepanja nadaljnjih dogovorov o podizvajanju, če so izpolnjeni naslednji kumulativni pogoji:

– predvideni podizvajalec je tretji ponudnik storitev IKT ali podizvajalec storitev IKT s sedežem v tretji državi in ▌nima ***podjetja, ustanovljenega v Uniji v skladu z zakonodajo države članice***;

– oddaja v podizvajanje se nanaša na kritično ali pomembno funkcijo finančnega subjekta;

– ***oddaja v podizvajanje bo povzročila resna in očitna tveganja za finančni subjekt ali finančno stabilnost finančnega sistema Unije.***

1b. Pooblastila iz odstavkov 1 in 1a se po potrebi izvajajo v zvezi s storitvami IKT, ki podpirajo nekritične ali pomembne funkcije, ki jih zagotavlja ključni tretji ponudnik storitev IKT.

1c. Glavni nadzornik in skupni nadzorni organ pri izvajanju pooblastil iz odstavkov 1 in 1a tega člena ustrezno upoštevata okvir, vzpostavljen z Direktivo (EU) 2016/1148, in se po potrebi posvetujeta z ustreznimi pristojnimi organi, ustanovljenimi z navedeno direktivo, da se prepreči nepotrebno podvajanje tehničnih in organizacijskih ukrepov, ki bi se lahko uporabljali za ključne tretje ponudnike storitev IKT v skladu z navedeno direktivo.

2. ***Skupni nadzorni organ pred dokončanjem in izdajo priporočil v skladu z odstavkom 1a obvesti ključnega tretjega ponudnika storitev IKT o njegovih namerah in mu omogoči predložitev informacij, za katere slednji razumno meni, da bi jih bilo treba upoštevati, preden se priporočilo dokonča, ali da izpodbija načrtovana priporočila. Razlogi za izpodbijanje priporočila so lahko med drugim, da bi prišlo do nesorazmernih motenj ali učinka na stranke, za katere ta uredba ne velja, ali da obstaja uspešnejša ali učinkovitejša rešitev za obvladovanje ugotovljenega tveganja.***

3. Ključni tretji ponudniki storitev IKT v dobri veri sodelujejo z glavnim nadzornikom in ***skupnim nadzornim organom*** in ***jima*** pomagajo pri izpolnjevanju ***njunih*** nalog.

4. Glavni nadzornik ***se*** lahko ***v primeru popolnega ali delnega neizpolnjevanja ukrepov, ki jih je treba sprejeti v skladu s točko (a), (b) ali (c) odstavka 1, in po izteku najmanj 60 koledarskih dni od datuma, ko je ključni tretji ponudnik storitev IKT prejel obvestilo o ukrepu, odloči, da*** naloži periodično denarno kazen, da ključnega tretjega ponudnika storitev IKT prisili ***k izpolnjevanju ukrepov***.

4a. Periodično denarno kazen iz odstavka 4 glavni nadzornik naloži le v skrajnem

primeru in v primerih, ko ključni tretji ponudnik storitev IKT ne izpolni ukrepov, ki jih je treba sprejeti v skladu s točko (a), (b) ali (c) odstavka 1.

5. Periodična denarna kazen iz odstavka 4 se naloži za vsak dan, dokler ni dosežena skladnost, vendar največ za šestmesečno obdobje po posredovanju obvestila ključnemu tretjemu ponudniku storitev IKT.

6. Znesek periodične denarne kazni, izračunan od datuma, določenega v odločbi o uvedbi periodične denarne kazni, je ***največ*** 1 % povprečnega dnevnega svetovnega prometa ključnega tretjega ponudnika storitev IKT***, povezanega s storitvami, zagotovljenimi finančnim subjektom, ki jih pokriva ta uredba,*** v prejšnjem obračunskem letu.

7. Denarna kazen je upravne narave in je izvršljiva. Izvršbo urejajo pravila civilnega postopka, ki veljajo v državi članici, na ozemlju katere se izvajajo inšpekcijski pregledi in obiski. Sodišča zadevne države članice so pristojna za pritožbe v zvezi z nepravilnim izvajanjem izvršbe. Zneski denarnih kazni se dodelijo splošnemu proračunu Evropske unije.

8. Evropski nadzorni organi javnosti razkrijejo vsako periodično denarno kazen, ki je bila naložena, razen če bi tako razkritje javnosti resno ogrozilo finančne trge ali povzročilo nesorazmerno škodo udeleženim stranem.

9. Pred naložitvijo periodične denarne kazni iz odstavka 4 da glavni nadzornik predstavnikom ključnega tretjega ponudnika storitev IKT, ki je predmet postopka, možnost, da podajo izjavo glede ugotovitev, in svoje odločitve utemelji le na ugotovitvah, na katere je imel ključni tretji ponudnik storitev IKT, ki je predmet postopke, priložnost podati pripombe. V postopku se v celoti spoštujejo pravice do obrambe oseb, ki so predmet postopka. Upravičene so do vpogleda v spis, ob upoštevanju zakonitega interesa drugih oseb za zaščito njihovih poslovnih skrivnosti. Pravica dostopa do spisa ne velja za zaupne informacije ali notranje pripravljalne dokumente glavnega nadzornika.

Člen 32

Zahteva po predložitvi informacij

1. Glavni nadzornik lahko s preprostim zahtevkom ali odločitvijo zahteva, da ključni tretji ponudniki storitev IKT zagotovijo vse informacije, ki so potrebne, da lahko glavni nadzornik opravlja svoje naloge v skladu s to uredbo, vključno z vsemi ustreznimi poslovnimi ali operativnimi dokumenti, pogodbami, dokumentacijo o politikah, revizijskimi poročili o varnosti IKT, poročili o incidentih, povezanih z IKT, ter vse informacije v zvezi s stranmi, ki jim je ključni tretji ponudnik storitev IKT oddal operativne funkcije ali dejavnosti v zunanje izvajanje.

   Od ključnih tretjih ponudnikov storitev IKT se zahteva le, da zagotovijo informacije iz prvega pododstavka v zvezi s storitvami, ki jih zagotavljajo finančnim subjektom, ki so predmet te uredbe in ki storitve ključnih tretjih ponudnikov storitev IKT uporabljajo za kritične ali pomembne funkcije. Ključni tretji ponudniki storitev IKT obvestijo zadevni finančni subjekt o zahtevah, ki se nanj nanašajo.

2. Pri pošiljanju preprostega zahtevka za informacije iz odstavka 1 glavni nadzornik:

   (a) navede sklic na ta člen kot pravno podlago za zahtevek;

   (b) navede namen zahtevka;

(c) natančno opredeli, katere informacije se zahteva;

(d) določi rok, do katerega je treba predložiti informacije;

(e) obvesti predstavnika ključnega tretjega ponudnika storitev IKT, od katerega se zahtevajo informacije, da mu ni zavezan posredovati informacij, vendar v primeru prostovoljnega odgovora na zahtevek posredovane informacije ne smejo biti napačne ali zavajajoče.

3. ***Kadar z odločitvijo zahteva predložitev*** informacij iz odstavka 1**,** glavni nadzornik:

(a) navede sklic na ta člen kot pravno podlago za zahtevek;

(b) navede namen zahtevka;

(c) natančno opredeli, katere informacije se zahteva;

(d) določi ***razumni*** rok, do katerega je treba predložiti informacije;

(e) navede periodične denarne kazni, določene v členu 31(4), če so zahtevane informacije, ki se predložijo, nepopolne ***ali če niso predložene v roku, določenem v točki (d)***;

(f) opozori na pravico do pritožbe zoper sklep pri odboru ESA za pritožbe ter pravico, da odločitev pregleda Sodišče Evropske unije (v nadaljnjem besedilu: Sodišče) v skladu s členoma 60 in 61 Uredbe (EU) št. 1093/2010, (EU) št. 1094/2010 oziroma (EU) št. 1095/2010.

4. Predstavniki ključnih tretjih ponudnikov storitev IKT predložijo zahtevane informacije. Pooblaščeni odvetniki lahko predložijo informacije v imenu svojih strank. Ključni tretji ponudniki storitev IKT so kljub temu v celoti odgovorni, če so predložene informacije nepopolne, napačne ali zavajajoče.

5. Glavni nadzornik nemudoma pošlje kopijo odločitve o posredovanju informacij pristojnim organom finančnih subjektov, ki uporabljajo storitve ključnih tretjih ponudnikov storitev IKT.

Člen 33

Splošne preiskave

1. Za namene izvajanja nalog iz te uredbe lahko glavni nadzornik ob pomoči pregledniške ekipe iz člena ***35***(1) opravi potrebne preiskave tretjih ponudnikov storitev IKT ***v skladu z načelom sorazmernosti***. ***Glavni nadzornik pri izvajanju preiskav ravna previdno in zagotovi, da so zaščitene pravice strank ključnih tretjih ponudnikov storitev IKT, ki niso predmet te uredbe, tudi v zvezi z učinkom na raven storitev, razpoložljivostjo podatkov in zaupnostjo.***

2. Glavni nadzornik ima pooblastila, da:

(a) preuči evidence, podatke, postopke in vse drugo gradivo, relevantno za izvajanje njegovih nalog, ne glede na vrsto nosilca podatkov, na katerem so shranjeni;

(b) ***na varen način pregleda*** dokumentacijo, podatke, postopke ali drugo gradivo ali pridobi njihove overjene kopije ali izpiske;

(c) pozove predstavnike tretjih ponudnikov storitev IKT, naj zagotovijo ustna ali pisna pojasnila glede dejstev ali dokumentov, povezanih s predmetom in namenom preiskave, ter zabeleži njihove odgovore;

(d) opravi razgovor z drugimi fizičnimi ali pravnimi osebami, ki privolijo v razgovor za namen zbiranja informacij o predmetu preiskave;

(e) zahteva evidence o telefonskem in podatkovnem prometu.

3. Uradniki in druge osebe, ki jih glavni nadzornik pooblasti za namene preiskave iz odstavka 1, svoja pooblastila izvajajo ob predložitvi pisnega pooblastila, v katerem sta navedena predmet in namen preiskave.

V pooblastilu so navedene tudi periodične denarne kazni iz člena 31(4), ki se naložijo, kadar zahtevane evidence, podatki, postopki ali katero koli drugo gradivo ali odgovori na vprašanja, zastavljena predstavnikom tretjega ponudnika storitev IKT, niso posredovani ali so nepopolni.

4. Predstavniki tretjih ponudnikov storitev IKT morajo privoliti v preiskave, ki jih z odločitvijo odredi glavni nadzornik. V odločitvi se navedejo predmet in namen preiskave, periodične denarne kazni iz člena 31(4), pravna sredstva, ki so na voljo na podlagi uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010, ter pravica, da odločitev pregleda Sodišče.

5. Glavni nadzorniki pravočasno pred preiskavo o njej in o identiteti pooblaščenih oseb obvesti pristojne organe finančnih subjektov, ki uporabljajo zadevnega tretjega ponudnika storitev IKT.

Člen 34

Inšpekcijski pregledi na kraju samem

1. Glavni nadzornik lahko za opravljanje nalog iz te uredbe ob pomoči pregledniških ekip iz člena 35(1) vstopi v vse poslovne prostore, na zemljišča ali nepremičnine tretjih ponudnikov storitev IKT, kot so sedež podjetja, operativni centri ter sekundarne lokacije, in tam izvede vse potrebne inšpekcijske preglede na kraju samem ali pa inšpekcijske preglede izvede na daljavo.

Pooblastilo za izvajanje inšpekcijskih pregledov na kraju samem iz prvega pododstavka ni omejeno na lokacije v Uniji, če inšpekcijski pregled lokacije v tretji državi izpolnjuje vse naslednje zahteve:

- ***glavni nadzornik mora opravljati svoje naloge v skladu s to uredbo;***
- ***pregled je neposredno povezan z zagotavljanjem storitev IKT finančnim subjektom Unije;***
- ***je pomemben za preiskavo, ki je v teku.***

1a. Skupni nadzorni izvršni organ pri inšpekcijskem pregledu na kraju samem prek glavnega nadzornika ravna previdno in zagotovi, da so zaščitene pravice ključnih tretjih ponudnikov storitev IKT, ki niso predmet te uredbe, tudi v zvezi z učinkom na raven storitev, z razpoložljivostjo podatkov in zaupnostjo.

2. Uradniki in druge osebe, ki jih glavni nadzornik pooblasti za izvajanje inšpekcijskega pregleda na kraju samem, lahko vstopijo v vse take poslovne prostore, na zemljišča ali nepremičnine in imajo vsa pooblastila, da zapečatijo vse poslovne prostore ter poslovne knjige ali evidence za trajanje in v obsegu, ki sta potrebna za izvedbo inšpekcijskega pregleda.

Svoja pooblastila izvajajo ob predložitvi pisnega pooblastila, ki podrobno določa

predmet in namen preiskave ter periodične denarne kazni iz člena 31(4), če predstavniki zadevnih tretjih ponudnikov storitev IKT ne privolijo v inšpekcijski pregled.

3. Glavni nadzorniki pravočasno pred inšpekcijskim pregledom obvestijo pristojne organe finančnih subjektov, ki uporabljajo zadevnega tretjega ponudnika storitev IKT.

4. Inšpekcijski pregledi zajemajo celoten sklop relevantnih sistemov, omrežij, naprav, informacij in podatkov na področju IKT***, za katere glavni nadzornik meni, da so ustrezni in pomembni s tehnološkega vidika, ter*** se uporabljajo za zagotavljanje storitev finančnim subjektom ali prispevajo k njihovemu zagotavljanju.

5. Pred ***načrtovano inšpekcijo*** na kraju samem glavni nadzorniki o njej dovolj zgodaj obvestijo ključne tretje ponudnike storitev IKT, razen če tako obvestilo ni mogoče zaradi izrednih ali kriznih razmer ali če bi privedlo do situacije, ko inšpekcijski pregled ali revizija ne bi bila več učinkovita.

6. Ključni tretji ponudnik storitev IKT privoli v inšpekcijski pregled na kraju samem, ki ga z odločitvijo odredi glavni nadzornik. V odločitvi se navedeta predmet in namen preiskave, določi datum, ko se bo ta začela, in navedejo periodične denarne kazni iz člena 31(4), pravna sredstva, ki so na voljo na podlagi uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010, ter pravica, da odločitev pregleda Sodišče.

7. Kadar uradniki in druge osebe, ki jih pooblasti glavni nadzornik, ugotovijo, da ključni tretji ponudnik storitev IKT nasprotuje inšpekcijskemu pregledu, ki je bil odrejen v skladu s tem členom, glavni nadzornik ključnega ***tretjega*** ponudnika storitev IKT obvesti o posledicah takega nasprotovanja, vključno z možnostjo, da pristojni organi ustreznih finančnih subjektov prekinejo pogodbene dogovore, sklenjene z navedenim ključnim tretjim ponudnikom storitev IKT.

Člen 35

Stalni nadzor

1. Glavnim nadzornikom pri izvajanju splošnih preiskav ali inšpekcijskih pregledov na kraju samem pomaga skupna pregledniška ekipa, vzpostavljena za vsakega ključnega tretjega ponudnika storitev IKT.

2. Skupna pregledniška ekipa iz odstavka 1 je sestavljena iz članov osebja glavnega nadzornika***, iz drugih evropskih nadzornih organov*** in ustreznih pristojnih organov, ki nadzorujejo finančne subjekte, ki jim ključni tretji ponudnik storitev IKT zagotavlja storitve, pri čemer ima ekipa največ deset članov, ki sodelujejo pri pripravi in izvajanju nadzornih dejavnosti. Vsi člani skupne pregledniške ekipe imajo strokovno znanje o tveganjih na področju IKT in operativnih tveganjih. Delovanje skupne pregledniške ekipe usklajuje imenovani uslužbenec evropskega nadzornega organa (v nadaljnjem besedilu: koordinator glavnega nadzornika).

3. Evropski nadzorni organi prek Skupnega odbora pripravijo skupne osnutke regulativnih tehničnih standardov, da natančneje določijo imenovanje članov skupne pregledniške ekipe, ki prihajajo iz ustreznih pristojnih organov, ter naloge in delovne dogovore pregledniške ekipe. Evropski nadzorni organi te osnutke regulativnih tehničnih standardov Komisiji predložijo do [UL: vstaviti datum eno leto po datumu začetka veljavnosti].

Na Komisijo se prenese pooblastilo za sprejetje regulativnih tehničnih standardov iz prvega pododstavka v skladu s členi 10 do 14 Uredbe (EU) št. 1093/2010, (EU)

št. 1094/2010 oziroma (EU) št. 1095/2010.

4. ***Skupni nadzorni organ*** v treh mesecih po zaključku preiskave ali inšpekcijskega pregleda na kraju samem sprejme priporočila, ki jih naslovi na ključnega tretjega ponudnika storitev IKT v skladu s pooblastili iz člena 31.

5. Priporočila iz odstavka 4 se nemudoma posredujejo ključnemu tretjemu ponudniku storitev IKT in pristojnim organom finančnih subjektov, ki jim zagotavlja storitve.

   Za namene izvajanja nadzornih dejavnosti lahko glavni nadzorniki ***in skupni nadzorni organ*** upoštevajo vsa ustrezna certificiranja, ki jih opravijo tretje osebe, in notranja ali zunanja revizijska poročila tretjih oseb na področju IKT, ki jih predloži ključni tretji ponudnik storitev IKT.

Člen 36

Usklajevanje pogojev, ki omogočajo izvajanje nadzora

1. Evropski nadzorni organi prek Skupnega odbora pripravijo osnutke regulativnih tehničnih standardov, da določijo:

   (a) informacije, ki jih mora predložiti ključni tretji ponudnik storitev IKT v prošnji za prostovoljno vključitev iz člena 28(8);

   (b) vsebino in obliko poročil, ki se lahko zahtevajo za namene točke (c) člena 31(1);

   (c) predstavitev informacij, vključno s strukturo, formati in metodami, ki jih mora ključni tretji ponudnik storitev IKT predložiti, razkriti ali poročati o njih v skladu s členom 31(1);

   (d) podrobnosti ocene pristojnih organov o ukrepih, ki so jih sprejeli ključni tretji ponudniki storitev IKT na podlagi priporočil ***skupnega nadzornega organa*** v skladu s členom 37(2).

2. Evropski nadzorni organi te osnutke regulativnih tehničnih standardov Komisiji predložijo do 1. januarja 20xx [UL: vstaviti datum eno leto po datumu začetka veljavnosti].

   Na Komisijo se prenese pooblastilo za dopolnitev te uredbe s sprejetjem regulativnih tehničnih standardov iz prvega pododstavka v skladu s postopkom iz členov 10 do 14 Uredbe (EU) št. 1093/2010, (EU) št. 1095/2010 oziroma (EU) št. 1094/2010.

Člen 37

Nadaljnje spremljanje s strani pristojnih organov

1. V 30 koledarskih dneh po prejemu priporočil, ki jih ***izda skupni nadzorni organ*** v skladu s členom 31(***1a***), ***ga*** ključni tretji ponudniki storitev IKT ▌obvestijo, ali nameravajo ta priporočila upoštevati. ***Skupni nadzorni organ*** te informacije takoj ***posreduje*** pristojnim organom ***zadevnih finančnih subjektov***.

2. Pristojni organi ***obvestijo finančne subjekte, ki so sklenili pogodbene dogovore s ključnimi tretjimi ponudniki storitev IKT, o tveganjih, opredeljenih v priporočilih, ki jih je skupni nadzorni organ pripravil za te ključne tretje ponudnike storitev IKT v skladu s členom 31(1a), in*** spremljajo, ali finančni subjekti upoštevajo opredeljena tveganja. ***Skupni nadzorni organ spremlja, ali so ključni tretji ponudniki IKT***

obravnavali tveganja, opredeljena v teh priporočilih.

3. ***Kadar regulativnih ciljev ni mogoče zagotoviti z drugimi ukrepi in so pristojni nacionalni organi na podlagi informacij, ki jih je sporočil skupni nadzorni odbor, zadevnim finančnim subjektom izdali opozorila, lahko upravni odbor glavnega nadzornika na priporočilo skupnega nadzornega organa in po posvetovanju s pristojnimi organi prizadetih finančnih subjektov odloči, da bo začasno delno ali v celoti prekinil uporabo ali uvedbo storitve, ki se zagotavlja finančnim subjektom, izpostavljenim tveganjem, opredeljenim v priporočilih za*** ključne tretje ponudnike storitev IKT***, dokler ta tveganja ne bodo ustrezno obravnavana***. Po potrebi ***in v skrajni sili*** lahko od ***ključnih tretjih ponudnikov storitev IKT*** zahtevajo, da delno ali v celoti prekinejo ustrezne pogodbene dogovore, sklenjene s ***finančnimi subjekti, ki so izpostavljeni opredeljenim tveganjem***.

4. Pri sprejemanju odločitev iz odstavka 3 ***odbor glavnega nadzornika upošteva*** vrsto in obseg tveganja, ki ga ključni tretji ponudnik storitev IKT ne obravnava, ter resnost neskladnosti, ob upoštevanju naslednjih meril:

   (a) resnost in trajanje neskladnosti;

   (b) ali je neskladnost razkrila resne pomanjkljivosti v postopkih, sistemih upravljanja, upravljanju tveganj in notranjih kontrolah ključnega tretjega ponudnika storitev IKT;

   (c) ali je neskladnost omogočila, povzročila ali drugače prispevala k finančnemu kriminalu;

   (d) ali je neskladnost storjena namerno ali iz malomarnosti;

   (da) ali začasna prekinitev ali ukinitev pomeni tveganje za neprekinjeno poslovanje uporabnika storitev ključnega tretjega ponudnika storitev IKT.

4a. Odločitve iz odstavka 3 se izvedejo šele, ko so o njih ustrezno obveščeni vsi prizadeti finančni subjekti. Prizadetim finančnim subjektom se zagotovi obdobje, ki ne presega tega, kar je nujno potrebno, da lahko svoje zunanje in pogodbene dogovore s ključnimi tretjimi ponudniki storitev IKT prilagodijo tako, da ne ogrožajo digitalne operativne odpornosti, ter da izvedejo svoje izhodne strategije in načrte prehoda iz člena 25.

Ključni tretji ponudniki storitev IKT, ki so predmet odločitev iz odstavka 3, v celoti sodelujejo s prizadetimi finančnimi subjekti.

5. Pristojni organi redno obveščajo ***skupni nadzorni organ*** o pristopih in ukrepih, sprejetih pri njihovih nadzornih nalogah v zvezi s finančnimi subjekti.

Člen 38

Nadomestila za nadzor

1. Evropski nadzorni organi ključnim tretjim ponudnikom storitev IKT zaračunajo nadomestila, ki v celoti pokrivajo potrebne izdatke evropskih nadzornih organov v zvezi z izvajanjem nalog nadzora v skladu s to uredbo, vključno s povračilom stroškov, ki lahko izhajajo iz opravljanja dela pristojnih organov, ki sodelujejo pri nadzornih dejavnostih v skladu s členom 35.

   Znesek nadomestila, ki se zaračuna ključnemu tretjemu ponudniku storitev IKT, krije vse ▌ stroške***, ki nastanejo zaradi izvajanja nalog iz tega oddelka,*** in je sorazmeren z

njegovim prometom.

1a. Če je z regulativnim in nadzornim organom tretje države sklenjen upravni dogovor v skladu z odstavkom 1 tega člena, je lahko ta organ del pregledniške ekipe iz člena 35(1).

2. Na Komisijo se prenese pooblastilo za sprejetje delegiranega akta v skladu s členom 50 za dopolnitev te uredbe z določitvijo višine nadomestil in načina njihovega plačila.

Člen 39

Mednarodno sodelovanje

1. EBA, ESMA in EIOPA lahko v skladu s členom 33 Uredbe (EU) št. 1093/2010, (EU) št. 1094/2010 oziroma (EU) št. 1095/2010 sklepajo upravne dogovore z regulativnimi in nadzornimi organi tretjih držav za spodbujanje mednarodnega sodelovanja v zvezi s tveganji tretjih oseb na področju IKT v različnih finančnih sektorjih, zlasti z razvojem dobrih praks za pregled praks in kontrol za upravljanje tveganj na področju IKT, blažilnih ukrepov in odzivov na incidente.

2. Evropski nadzorni organi prek Skupnega odbora Evropskemu parlamentu, Svetu in Komisiji vsakih pet let predložijo skupno zaupno poročilo, ki povzema ugotovitve ustreznih razprav z organi tretjih držav iz odstavka 1, pri čemer je poudarek na razvoju tveganj tretjih oseb na področju IKT in posledicah za finančno stabilnost, celovitost trga, zaščito vlagateljev ali delovanje enotnega trga.

POGLAVJE VI

DOGOVORI O IZMENJAVI INFORMACIJ

Člen 40

Dogovori o izmenjavi informacij in obveščevalnih podatkov o kibernetskih grožnjah

1. Finančni subjekti si ***prizadevajo za izmenjavo informacij in obveščevalnih podatkov*** o kibernetskih grožnjah ***med seboj in s tretjimi ponudniki storitev IKT***, vključno s kazalniki ogroženosti, taktikami, tehnikami in postopki, opozorili glede kibernetske varnosti in orodji za konfiguracijo, če taka izmenjava informacij in obveščevalnih podatkov:

   (a) stremi k povečanju digitalne operativne odpornosti finančnih subjektov ***in tretjih ponudnikov storitev IKT***, zlasti z ozaveščanjem v zvezi s kibernetskimi grožnjami, k omejevanju ali oviranju zmožnosti širjenja kibernetskih groženj ter podpiranju ▌obrambnih zmogljivosti, tehnik odkrivanja groženj, blažilnih ukrepov ali faz odzivanja in okrevanja ▌;

   (b) poteka v zaupanja vrednih skupnostih finančnih subjektov ***in tretjih ponudnikov storitev IKT***;

   (c) se izvaja z dogovori o izmenjavi informacij, ki ščitijo potencialno občutljivo naravo izmenjanih informacij in ki jih urejajo pravila ravnanja ob polnem spoštovanju poslovne zaupnosti, varstva osebnih podatkov[28] in smernic o politiki konkurence[29].

2. Za namene točke (c) odstavka 1 dogovori o izmenjavi informacij opredeljujejo pogoje za sodelovanje in, kjer je to ustrezno, določajo podrobnosti o sodelovanju javnih organov in vlogi, v kateri so lahko slednji povezani z dogovori o izmenjavi informacij, ter o operativnih elementih, vključno z uporabo namenskih informacijskih platform.

3. Finančni subjekti obvestijo pristojne organe o svojem sodelovanju pri dogovorih o izmenjavi informacij iz odstavka 1 po potrditvi njihovega članstva ali, kjer je to ustrezno, o prenehanju članstva, ko slednje začne veljati.

[28] V skladu z Uredbo (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).

[29] Sporočilo Komisije – Smernice o uporabi člena 101 Pogodbe o delovanju Evropske unije za sporazume o horizontalnem sodelovanju, 2011/C 11/01.

POGLAVJE VII

PRISTOJNI ORGANI

Člen 41

Pristojni organi

Brez poseganja v določbe o okviru nadzora za ključne tretje ponudnike storitev IKT iz oddelka II poglavja V te uredbe izpolnjevanje obveznosti iz te uredbe zagotavljajo pristojni organi v skladu s pooblastili, podeljenimi z ustreznimi pravnimi akti, in sicer:

(a) za kreditne institucije pristojni organ, imenovan v skladu s členom 4 Direktive 2013/36/EU, brez poseganja v posebne naloge, prenesene na ECB z Uredbo (EU) št. 1024/2013;

(b) za ponudnike plačilnih storitev pristojni organ, imenovan v skladu s členom 22 Direktive (EU) 2015/2366;

(c) za institucije za izdajo elektronskega denarja pristojni organ, imenovan v skladu s členom 37 Direktive 2009/110/ES;

(d) za investicijska podjetja pristojni organ, imenovan v skladu s členom 4 Direktive (EU) 2019/2034;

(e) za ponudnike storitev v zvezi s kriptoimetji, izdajatelje ***in ponudnike*** kriptoimetij, izdajatelje ***in ponudnike*** žetonov, vezanih na sredstva, in izdajatelje pomembnih žetonov, vezanih na sredstva, pristojni organ, imenovan v skladu s prvo alineo točke (ee) člena 3(1) [Uredbe (EU) 20xx, uredba MiCA];

(f) za centralne depotne družbe ***in operaterje sistemov poravnave vrednostnih papirjev*** pristojni organ, imenovan v skladu s členom 11 Uredbe (EU) št. 909/2014;

(g) za centralne nasprotne stranke pristojni organ, imenovan v skladu s členom 22 Uredbe (EU) št. 648/2012;

(h) za mesta trgovanja in izvajalce storitev sporočanja podatkov pristojni organ, imenovan v skladu s členom 67 Direktive 2014/65/EU;

(i) za repozitorije sklenjenih poslov pristojni organ, imenovan v skladu s členom 55 Uredbe (EU) št. 648/2012;

(j) za upravitelje alternativnih investicijskih skladov pristojni organ, imenovan v skladu s členom 44 Direktive 2011/61/EU;

(k) za družbe za upravljanje pristojni organ, imenovan v skladu s členom 97 Direktive 2009/65/ES;

(l) za zavarovalnice in pozavarovalnice pristojni organ, imenovan v skladu s členom 30 Direktive 2009/138/ES;

(m) za zavarovalne posrednike, pozavarovalne posrednike in posrednike dopolnilnih zavarovanj pristojni organ, imenovan v skladu s členom 12 Direktive (EU) 2016/97;

(n) za institucije za ***zagotavljanje poklicnega pokojninskega zavarovanja*** pristojni

organ, imenovan v skladu s členom 47 Direktive 2016/2341/ES;

(o) za bonitetne agencije pristojni organ, imenovan v skladu s členom 21 Uredbe (ES) št. 1060/2009;

(p) za zakonite revizorje in revizijska podjetja pristojni organ, imenovan v skladu s členoma 3(2) in 32 Direktive 2006/43/ES;

(q) za upravljavce ključnih referenčnih vrednosti pristojni organ, imenovan v skladu s členoma 40 in 41 Uredbe ***(EU) 20161011***;

(r) za ponudnike storitev množičnega financiranja pristojni organ, imenovan v skladu s členom ***29*** Uredbe ***(EU) 2020/1503***;

(s) za repozitorije listinjenj pristojni organ, imenovan v skladu s členoma 10 in 14(1) Uredbe (EU) št. 2017/2402.

Člen 42

Sodelovanje z ustanovami in organi, ustanovljenimi z Direktivo (EU) 2016/1148

1. Za spodbujanje sodelovanja in omogočanje nadzornih izmenjav med pristojnimi organi, imenovanimi na podlagi te uredbe, in skupino za sodelovanje, ustanovljeno s členom 11 Direktive (EU) 2016/1148, ***so*** evropski nadzorni organi in pristojni organi ***povabljeni k sodelovanju pri*** delu skupine za sodelovanje***, če to delo zadeva dejavnosti nadzora oziroma pregleda v zvezi s subjekti iz točke 7 Priloge II k Direktivi (EU) 2016/1148, ki so bili prav tako opredeljeni kot ključni tretji ponudniki storitev IKT v skladu s členom 28 te uredbe.***

2. Pristojni organi se lahko po potrebi posvetujejo z enotno kontaktno točko in nacionalnimi skupinami za odzivanje na incidente na področju računalniške varnosti iz člena 8 oziroma 9 Direktive (EU) 2016/1148.

2a. Glavni nadzornik obvesti pristojne organe, imenovane na podlagi Direktive (EU) 2016/1148, in z njimi sodeluje pred izvedbo splošnih preiskav in inšpekcijskih pregledov na kraju samem v skladu s členi 33 in 34 te uredbe.

Člen 43

Finančne medsektorske vaje, obveščanje in sodelovanje

1. Evropski nadzorni organi lahko prek Skupnega odbora in v sodelovanju s pristojnimi organi, ECB, ***enotnim odborom za reševanje v zvezi s subjekti, ki spadajo v Uredbo (EU) št. 806/2014***, in ESRB vzpostavijo mehanizme, ki omogočajo izmenjavo učinkovitih praks med finančnimi sektorji za povečanje situacijskega zavedanja in prepoznavanje skupnih kibernetskih ranljivosti in tveganj med sektorji.

   Oblikujejo lahko vaje za krizno upravljanje in izredne razmere, ki vključujejo scenarije kibernetskih napadov, da bi razvili komunikacijske kanale in postopoma omogočili učinkovit usklajen odziv na ravni EU v primeru večjega čezmejnega incidenta, povezanega z IKT, ali ***večje kibernetske*** grožnje, ki bi imela sistemski učinek na celotni finančni sektor Unije.

   S temi vajami se lahko po potrebi testira tudi odvisnost finančnega sektorja od drugih

gospodarskih sektorjev.

2. Pristojni organi, EBA, ESMA ali EIOPA, ECB***, nacionalni organi za reševanje in Enotni odbor za reševanje*** tesno sodelujejo ***v zvezi z informacijami o subjektih, ki spadajo na področje Uredbe (EU) št. 806/2014,*** in si izmenjujejo informacije za izvajanje svojih nalog v skladu s členi 42 do 48. Tesno usklajujejo svoj nadzor, da bi opredelili in odpravili kršitve te uredbe, razvili in spodbujali dobre prakse, olajšali sodelovanje, spodbujali usklajeno razlago in zagotavljali ocene med jurisdikcijami v primeru nesoglasij.

Člen 44

Upravne kazni in popravni ukrepi

1. Pristojni organi imajo vsa pooblastila za nadzor, preiskovanje in izrekanje sankcij, potrebna za izpolnjevanje njihovih nalog v skladu s to uredbo.

2. Pooblastila iz odstavka 1 zajemajo vsaj naslednja pooblastila:

   (a) dostop do katerega koli dokumenta ali podatkov v kakršni koli obliki, za katerega pristojni organ meni, da bi lahko bil pomemben za izvajanje njegovih nalog, ter prejem ali izdelava njegove kopije;

   (b) opravljanje inšpekcijskih pregledov ali preiskav na kraju samem;

   (c) zahtevanje obnovitvenih in popravnih ukrepov za kršitve zahtev te uredbe.

3. Brez poseganja v pravico držav članic, da naložijo kazenske sankcije v skladu s členom 46, države članice vzpostavijo pravila, ki določajo ustrezne upravne kazni in popravne ukrepe za kršitve te uredbe, ter zagotovijo njihovo učinkovito izvajanje.

Te kazni in ukrepi so učinkoviti, sorazmerni in odvračilni.

4. Države članice pristojne organe pooblastijo, da v primeru kršitev te uredbe uporabijo vsaj naslednje upravne kazni ali popravne ukrepe:

   (a) izdajo odredbo, ki od fizične ali pravne osebe zahteva, da preneha z zadevnim ravnanjem in da tega ravnanja več ne ponovi;

   (b) zahtevajo začasno ali trajno prenehanje prakse ali ravnanja, za katerega ***velja***, da je v nasprotju z določbami te uredbe, in preprečijo, da bi se taka praksa ali ravnanje ponovilo;

   (c) sprejmejo kakršenkoli ukrep, tudi denarni, za zagotovitev, da finančni subjekti še naprej izpolnjujejo zakonske zahteve;

   (d) kolikor to dovoljuje nacionalno pravo, zahtevajo obstoječe evidence o podatkovnem prometu, ki jih ima telekomunikacijski operater, kadar obstaja utemeljen sum kršitve te uredbe in kadar so lahko take evidence pomembne za preiskavo kršitev te direktive, in

   (e) izdajajo javna obvestila, vključno z javnimi izjavami, ki navajajo identiteto fizične ali pravne osebe in naravo kršitve.

5. Kadar se določbe iz točke (c) odstavka 2 in odstavka 4 uporabljajo za pravne osebe,

države članice na pristojne organe prenesejo pooblastilo, da v skladu s pogoji iz nacionalnega prava članom upravljalnega organa in drugim posameznikom, ki so v skladu z nacionalnim pravom odgovorni za kršitev, naložijo upravne kazni in popravne ukrepe.

6. Države članice zagotovijo, da je kakršna koli odločitev o naložitvi upravnih kazni ali popravnih ukrepov iz točke (c) odstavka 2 ustrezno obrazložena in da v zvezi z njo velja pravica do pritožbe.

Člen 45

Izvajanje pooblastil za nalaganje upravnih kazni in popravnih ukrepov

1. Pristojni organi izvajajo pooblastila za nalaganje upravnih kazni in popravnih ukrepov iz člena 44 v skladu s svojim nacionalnim pravnim okvirom, kot je ustrezno:

   (a) neposredno;

   (b) v sodelovanju z drugimi organi;

   (c) v okviru svoje pristojnosti s prenosom pooblastil na druge organe;

   (d) z vložitvijo zahtevka pri pristojnih sodnih organih.

2. Pristojni organi pri določitvi vrste in ravni upravne kazni ali popravnega ukrepa, naloženega na podlagi člena 44, upoštevajo, v kolikšni meri je kršitev namerna ali posledica malomarnosti ter vse druge zadevne okoliščine, po potrebi tudi:

   (a) pomen, resnost in trajanje kršitve;

   (b) stopnjo odgovornosti fizične ali pravne osebe, ki je odgovorna za kršitev;

   (c) finančno trdnost odgovorne fizične ali pravne osebe;

   (d) pomen pridobljenih dobičkov ali preprečenih izgub s strani odgovorne fizične ali pravne osebe, če jih je mogoče opredeliti;

   (e) izgube, ki so jih zaradi kršitve imele tretje osebe, če jih je mogoče določiti;

   (f) raven sodelovanja odgovorne fizične ali pravne osebe s pristojnim organom, brez poseganja v potrebo po zagotovitvi povračila pridobljenega dobička ali preprečene izgube te osebe na podlagi kršitve;

   (g) prejšnje kršitve odgovorne fizične ali pravne osebe.

Člen 46

Kazenske sankcije

1. Države članice lahko sklenejo, da ne bodo določile pravil o upravnih kaznih ali popravnih ukrepih za kršitve, za katere se v njihovem nacionalnem pravu uporabljajo kazenske sankcije.

2. Kadar države članice sklenejo določiti kazenske sankcije za kršitve te uredbe, zagotovijo, da so vzpostavljeni ustrezni ukrepi, na podlagi katerih imajo pristojni organi na voljo vsa potrebna pooblastila za sodelovanje s sodnimi organi, organi pregona ali pravosodnimi organi v njihovi jurisdikciji, da prejemajo specifične informacije,

povezane s kazenskimi preiskavami ali postopki, sproženimi ob kršitvah te uredbe, in da enake informacije zagotovijo drugim pristojnim organom ter EBA, ESMA ali EIOPA, da jim omogočijo izpolnitev njihove obveznosti sodelovanja za namene te uredbe.

Člen 47

Dolžnosti uradnega obveščanja

Države članice Komisijo, ESMA, EBA in EIOPA uradno obvestijo o zakonih in drugih predpisih za izvajanje tega poglavja, tudi o ustreznih kazenskopravnih določbah, do [UL: vstaviti datum ***12 mesecev*** po datumu začetka veljavnosti]. Komisijo, ESMA, EBA in EIOPA brez nepotrebnega odlašanja uradno obvestijo tudi o vseh poznejših spremembah teh zakonov in drugih predpisov.

Člen 48

Objava upravnih kazni

1. Pristojni organi na svojih uradnih spletiščih brez nepotrebnega odlašanja objavijo vsako odločitev o naložitvi upravne kazni, zoper katero ni pritožbe, potem ko je bil naslovnik kazni obveščen o navedeni odločitvi.

2. Objava iz odstavka 1 vsebuje informacije o vrsti in naravi kršitve, ***naloženih kaznih in izjemoma o*** identiteti odgovornih oseb ▌ .

3. Kadar pristojni organ po presoji vsakega posameznega primera meni, da bi bila objava identitete v primeru pravnih oseb ali identitete in osebnih podatkov v primeru fizičnih oseb nesorazmerna, da bi ogrozila stabilnost finančnih trgov ali nadaljevanje tekoče kazenske preiskave ali da bi, če je to mogoče ugotoviti, povzročila nesorazmerno škodo udeleženi osebi, sprejme eno od naslednjih rešitev v zvezi z odločitvijo o izreku upravne kazni:

   (a) odloži objavo, dokler ni več razlogov za neobjavo;

   (b) objavo izvede na anonimni podlagi v skladu z nacionalno zakonodajo ali

   (c) odločitve ne objavi, kadar možnosti iz točk (a) in (b) ne zadostujejo za zagotovitev odprave kakršne koli nevarnosti za stabilnost finančnih trgov ali kadar taka objava ne bi bila sorazmerna s prizanesljivostjo izrečene kazni.

4. V primeru odločitve, da se upravna kazen objavi na anonimni podlagi, kot je navedeno v točki (b) odstavka 3, se lahko objava ustreznih podatkov odloži.

5. Kadar pristojni organ objavi odločitev o naložitvi upravne kazni, zoper katero je mogoča pritožba pred ustreznimi sodnimi organi, pristojni organi na svojem uradnem spletišču nemudoma dodajo te informacije in vse poznejše povezane informacije o izidu take pritožbe. Objavijo se tudi vse sodne odločbe, s katerimi se razveljavi odločitev o naložitvi upravne kazni.

6. Pristojni organi zagotovijo, da vsaka objava iz odstavkov 1 do 4 ostane na njihovem uradnem spletišču najmanj pet let po objavi. Osebni podatki, vsebovani v objavi, se hranijo le na uradnem spletišču pristojnega organa, in sicer za obdobje, ki se zahteva v skladu z veljavnimi pravili o varstvu podatkov.

Člen 49

Poslovna skrivnost

1. Za vse zaupne informacije, prejete, izmenjane ali posredovane v skladu s to uredbo, veljajo pogoji poslovne skrivnosti iz odstavka 2.
2. Obveznost varovanja poslovne skrivnosti velja za vse osebe, ki so ali so bile zaposlene pri pristojnih organih iz te uredbe ali katerem koli organu ali tržnem podjetju ali fizični ali pravni osebi, na katero so navedeni pristojni organi prenesli svoja pooblastila, vključno z revizorji in strokovnjaki, katerih storitve so naročili.
3. Informacije, ki so poslovna skrivnost, se ne smejo razkriti nobeni drugi osebi ali organu, razen na podlagi določb prava Unije ali nacionalnega prava.
4. Vse informacije, ki si jih pristojni organi izmenjajo na podlagi te uredbe in ki zadevajo poslovne ali operativne razmere in druge gospodarske ali osebne zadeve, se štejejo za zaupne in zanje veljajo zahteve o varovanju poslovne skrivnosti, razen kadar pristojni organ v času posredovanja teh informacij navede, da se lahko razkrijejo, ali kadar je tako razkritje potrebno v sodnih postopkih.

POGLAVJE VIII

DELEGIRANI AKTI

Člen 50

Izvajanje prenosa pooblastila

1. Pooblastilo za sprejemanje delegiranih aktov je preneseno na Komisijo pod pogoji, določenimi v tem členu.

2. Pooblastilo za sprejetje delegiranih aktov iz členov 28(3) in 38(2) se prenese na Komisijo za petletno obdobje z začetkom od [UP: vstaviti datum pet let po datumu začetka veljavnosti te uredbe]. ***Komisija najpozneje devet mesecev pred koncem petletnega obdobja pripravi poročilo o prenosu pooblastila. Prenos pooblastila se samodejno podaljšuje za enako dolga obdobja, razen če Evropski parlament ali Svet nasprotuje temu podaljšanju najpozneje tri mesece pred koncem vsakega obdobja.***

3. Prenos pooblastila iz členov 28(3) in 38(2) lahko kadar koli prekliče Evropski parlament ali Svet. S sklepom o preklicu preneha veljati prenos pooblastila iz navedenega sklepa. Sklep začne učinkovati dan po objavi v Uradnem listu Evropske unije ali na poznejši dan, ki je določen v navedenem sklepu. Sklep ne vpliva na veljavnost že veljavnih delegiranih aktov.

4. Komisija se pred sprejetjem delegiranega akta posvetuje s strokovnjaki, ki jih imenujejo države članice, v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje.

5. Komisija takoj po sprejetju delegiranega akta o njem sočasno uradno obvesti Evropski parlament in Svet.

6. Delegirani akt, sprejet na podlagi členov 28(3) in 38(2), začne veljati le, če mu niti Evropski parlament niti Svet ne nasprotuje v roku ***treh*** mesecev od uradnega obvestila Evropskemu parlamentu in Svetu o tem aktu ali če pred iztekom tega roka tako Evropski parlament kot Svet obvestita Komisijo, da mu ne bosta nasprotovala. Ta rok se na pobudo Evropskega parlamenta ali Sveta podaljša za ***tri mesece***.

POGLAVJE IX

PREHODNE IN KONČNE DOLOČBE

ODDELEK I

Člen 51

Klavzula o pregledu

Komisija do [UP: vstaviti datum pet let po datumu začetka veljavnosti te uredbe] po posvetovanju z EBA, ESMA, EIOPA in ESRB po potrebi opravi pregled ter Evropskemu parlamentu in Svetu predloži poročilo ter mu po potrebi priloži zakonodajni predlog. ***Poročilo preveri vsaj naslednje:***

(a) možnost razširitve področja uporabe te uredbe na operaterje plačilnih sistemov;

(b) prostovoljnost poročanja o pomembnih kibernetskih grožnjah;

(c) merila za imenovanje ključnih tretjih ponudnikov storitev IKT iz člena 28(2) ***in***

(d) učinkovitost odločanja skupnega nadzornega organa in izmenjavo informacij med skupnim nadzornim organom in nečlani nacionalnih pristojnih organov.

ODDELEK II

SPREMEMBE

Člen 52

Spremembe Uredbe (ES) št. 1060/2009

V Prilogi I k Uredbi (ES) št. 1060/2009 se prvi pododstavek točke 4 oddelka A nadomesti z naslednjim:

„Bonitetna agencija ima ustrezne upravne in računovodske postopke, mehanizme notranjih kontrol, učinkovite postopke za ocenjevanje tveganj ter učinkovite kontrolne in zaščitne ukrepe za upravljanje sistemov IKT v skladu z Uredbo (EU) 2021/xx Evropskega parlamenta in Sveta* [DORA].

* Uredba (EU) 2021/xx Evropskega parlamenta in Sveta […] (UL L XX, DD.MM.LLLL, str. X).“

Člen 53

Spremembe Uredbe (EU) št. 648/2012

Uredba (EU) št. 648/2012 se spremeni:

(1) člen 26 se spremeni:

(a) odstavek 3 se nadomesti z naslednjim:

„ 3. CNS vzdržuje in upravlja organizacijsko strukturo, ki zagotavlja neprekinjenost in urejeno delovanje pri opravljanju njenih storitev in dejavnosti. Uporablja ustrezne in sorazmerne sisteme, vire in postopke, vključno s sistemi IKT, ki se upravljajo v skladu z Uredbo (EU) 2021/xx Evropskega parlamenta in Sveta* [DORA].

* Uredba (EU) 2021/xx Evropskega parlamenta in Sveta […] (UL L XX, DD.MM.LLLL, str. X).“;

(b) odstavek 6 se črta;

(2) člen 34 se spremeni:

(a) odstavek 1 se nadomesti z naslednjim:

„1. CNS vzpostavi, izvaja in vzdržuje ustrezno politiko neprekinjenega poslovanja in načrt ponovne vzpostavitve delovanja, ki vključuje načrt neprekinjenega poslovanja na področju IKT in načrt okrevanja IKT po katastrofi, vzpostavljena v skladu z Uredbo (EU) 2021/xx [DORA], katerih cilj je zagotoviti ohranjanje njenih funkcij, pravočasna obnovitev delovanja in izpolnitev obveznosti CNS.“;

(b) v odstavku 3 se prvi pododstavek nadomesti z naslednjim:

„Da se zagotovi dosledna uporaba tega člena, ESMA po posvetovanju s članicami ESCB pripravi osnutke regulativnih tehničnih standardov, ki določajo najmanjši obseg vsebine in minimalne zahteve za politiko neprekinjenega poslovanja in načrt ponovne vzpostavitve delovanja, razen načrta neprekinjenega poslovanja na področju IKT in načrta okrevanja IKT po katastrofi.“;

(3) v členu 56 se prvi pododstavek odstavka 3 nadomesti z naslednjim:

„3. Da se zagotovi dosledna uporaba tega člena, ESMA pripravi osnutke regulativnih tehničnih standardov, ki določajo podrobnosti v zvezi z vlogo za registracijo iz odstavka 1, razen za zahteve, povezane z upravljanjem tveganj na področju IKT.“;

(4) v členu 79 se odstavka 1 in 2 nadomestita z naslednjim:

„1. Repozitorij sklenjenih poslov opredeli vire operativnega tveganja in jih zmanjša na najnižjo raven tudi z razvojem ustreznih sistemov, kontrol in postopkov, vključno s sistemi IKT, ki se upravljajo v skladu z Uredbo (EU) 2021/xx [DORA].

2. Repozitorij sklenjenih poslov vzpostavi, izvaja in vzdržuje ustrezno politiko neprekinjenega poslovanja in načrt ponovne vzpostavitve delovanja, vključno z načrtom neprekinjenega poslovanja na področju IKT in načrtom okrevanja IKT po katastrofi, vzpostavljenima v skladu z Uredbo (EU) 2021/xx [DORA], katerih cilj je zagotoviti ohranjanje njegovih funkcij, pravočasno obnovitev delovanja in izpolnitev obveznosti repozitorija sklenjenih poslov.“;

(5) v členu 80 se črta odstavek 1.

Člen 54

Spremembe Uredbe (EU) št. 909/2014

Člen 45 Uredbe (EU) št. 909/2014 se spremeni:

(1) odstavek 1 se nadomesti z naslednjim:

„1. CDD odkriva notranje in zunanje vire operativnega tveganja in zmanjša njihov vpliv tudi z uporabo ustreznih orodij, postopkov in politik IKT, vzpostavljenih in upravljanih v skladu z Uredbo (EU) 2021/xx Evropskega parlamenta in Sveta* [DORA], ter z drugimi pomembnimi ustreznimi orodji, kontrolami in postopki za druge vrste operativnega tveganja, med drugim za vse sisteme poravnave vrednostnih papirjev, ki jih upravlja.

* Uredba (EU) 2021/xx Evropskega parlamenta in Sveta […] (UL L XX, DD.MM.LLLL, str. X).“;

(2) odstavek 2 se črta;

(3) odstavka 3 in 4 se nadomestita z naslednjim:

„3. CDD za storitve, ki jih opravlja, in vse sisteme poravnave vrednostnih papirjev, ki jih upravlja, vzpostavi, izvaja in vzdržuje ustrezno politiko neprekinjenega poslovanja in načrt ponovne vzpostavitve delovanja, vključno z načrtom neprekinjenega poslovanja na področju IKT in načrtom okrevanja IKT po katastrofi, vzpostavljenima v skladu z Uredbo (EU) 2021/xx [DORA], da v primeru dogodkov, za katere obstaja znatna nevarnost, da bodo povzročili motnje pri poslovanju, zagotovi ohranitev svojih storitev, pravočasno ponovno vzpostavitev poslovanja in izpolnjevanje svojih obveznosti.

4. Načrt iz odstavka 3 ob motnji poskrbi za obnovitev vseh poslov in pozicij udeležencev, da lahko udeleženci CDD še naprej poslujejo zanesljivo in poravnavo zaključijo na načrtovani datum, in sicer to omogoči tudi z zagotavljanjem, da lahko začnejo kritični sistemi informacijske tehnologije po motnji znova delovati, kot je določeno v odstavkih 5 in 7 člena 11 Uredbe

(EU) 2021/xx [DORA].“;

Člen 55

Spremembe Uredbe (EU) št. 600/2014

Uredba (EU) št. 600/2014 se spremeni:

(1) člen 27g se spremeni:

(a) odstavek 4 se črta;

(b) v odstavku 8 se točka (c) nadomesti z naslednjim:

(c) „(c) konkretne organizacijske zahteve iz odstavkov 3 in 5.“;

(2) člen 27h se spremeni:

(a) odstavek 5 se črta;

(b) v odstavku 8 se točka (e) nadomesti z naslednjim:

„(e) konkretne organizacijske zahteve iz odstavka 4.“;

(3) člen 27i se spremeni:

(a) odstavek 3 se črta;

(b) v odstavku 5 se točka (b) nadomesti z naslednjim:

„(b) konkretne organizacijske zahteve iz odstavkov 2 in 4.“

Člen 56

Začetek veljavnosti in uporaba

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

Uporablja se od [UP: vstaviti datum ***24*** mesecev po datumu začetka veljavnosti].

Člena 23 in 24 pa se uporabljata od [UP: vstaviti datum 36 mesecev po datumu začetka veljavnosti te uredbe].

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

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

V Bruslju,

Za Evropski parlament	*Za Svet*
Predsednik	*Predsednik*

POSTOPEK V PRISTOJNEM ODBORU

Naslov	Digitalna operativna odpornost za finančni sektor in sprememba uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014 in (EU) št. 909/2014
Referenčni dokumenti	COM(2020)0595 – C9-0304/2020 – 2020/0266(COD)
Datum predložitve EP	24.9.2020
Pristojni odbor Datum razglasitve na zasedanju	ECON 17.12.2020
Odbori, zaprošeni za mnenje Datum razglasitve na zasedanju	ITRE IMCO 17.12.2020 17.12.2020
Odbori, ki niso podali mnenja Datum sklepa	ITRE IMCO 15.10.2020 27.10.2020
Poročevalec/-ka Datum imenovanja	Billy Kelleher 15.10.2020
Obravnava v odboru	14.4.2021 14.6.2021
Datum sprejetja	1.12.2021
Izid končnega glasovanja	+: 44 –: 5 0: 5
Poslanci, navzoči pri končnem glasovanju	Gerolf Annemans, Gunnar Beck, Marek Belka, Isabel Benjumea Benjumea, Stefan Berger, Gilles Boyer, Engin Eroglu, Markus Ferber, Jonás Fernández, Raffaele Fitto, Frances Fitzgerald, Luis Garicano, Sven Giegold, Valentino Grant, Claude Gruffat, José Gusmão, Enikő Győri, Eero Heinäluoma, Danuta Maria Hübner, Stasys Jakeliūnas, France Jamet, Billy Kelleher, Ondřej Kovařík, Georgios Kircos (Georgios Kyrtsos), Aurore Lalucq, Philippe Lamberts, Aušra Maldeikienė, Pedro Marques, Kostas Mavridis (Costas Mavrides), Jörg Meuthen, Csaba Molnár, Siegfried Mureşan, Caroline Nagtegaal, Luděk Niedermayer, Levteris Nikolau-Alavanos (Lefteris Nikolaou-Alavanos), Lídia Pereira, Kira Marie Peter-Hansen, Sirpa Pietikäinen, Evelyn Regner, Antonio Maria Rinaldi, Alfred Sant, Martin Schirdewan, Joachim Schuster, Ralf Seekatz, Pedro Silva Pereira, Paul Tang, Irene Tinagli, Ernest Urtasun, Inese Vaidere, Johan Van Overtveldt, Stéphanie Yon-Courtin, Marco Zanni, Roberts Zīle
Namestniki, navzoči pri končnem glasovanju	Levteris Hristoforu (Lefteris Christoforou)
Datum predložitve	7.12.2021

POIMENSKO GLASOVANJE PRI KONČNEM GLASOVANJU V PRISTOJNEM ODBORU

44	+
ECR	Raffaele Fitto, Johan Van Overtveldt, Roberts Zīle
NI	Enikő Győri
PPE	Isabel Benjumea Benjumea, Stefan Berger, Levteris Hristoforu (Lefteris Christoforou), Markus Ferber, Frances Fitzgerald, Danuta Maria Hübner, Georgios Kircos (Georgios Kyrtsos), Aušra Maldeikienė, Siegfried Mureşan, Luděk Niedermayer, Lídia Pereira, Sirpa Pietikäinen, Ralf Seekatz, Inese Vaidere
Renew	Gilles Boyer, Engin Eroglu, Luis Garicano, Billy Kelleher, Ondřej Kovařík, Caroline Nagtegaal, Stéphanie Yon-Courtin
S&D	Marek Belka, Jonás Fernández, Eero Heinäluoma, Aurore Lalucq, Pedro Marques, Kostas Mavridis (Costas Mavrides), Csaba Molnár, Evelyn Regner, Alfred Sant, Joachim Schuster, Pedro Silva Pereira, Paul Tang, Irene Tinagli
Verts/ALE	Sven Giegold, Claude Gruffat, Stasys Jakeliūnas, Philippe Lamberts, Kira Marie Peter-Hansen, Ernest Urtasun

5	-
ID	Gerolf Annemans, Gunnar Beck, France Jamet, Jörg Meuthen
NI	Levteris Nikolau-Alavanos (Lefteris Nikolaou-Alavanos)

5	0
ID	Valentino Grant, Antonio Maria Rinaldi, Marco Zanni
The Left	José Gusmão, Martin Schirdewan

Uporabljeni znaki:
+ : za
- : proti
0 : vzdržani