EVROPSKA
KOMISIJA

Bruselj, 24.9.2020
COM(2020) 595 final

2020/0266 (COD)

Predlog

UREDBA 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)

{SEC(2020) 307 final} - {SWD(2020) 198 final} - {SWD(2020) 199 final}

OBRAZLOŽITVENI MEMORANDUM

1. OZADJE PREDLOGA

- Razlogi za predlog in njegovi cilji

Ta predlog je del svežnja o digitalnih financah, tj. svežnja ukrepov za nadaljnje omogočanje in podpiranje potenciala digitalnih financ v smislu inovacij in konkurence ter hkratno blaženje tveganj, ki izhajajo iz tega. V skladu s prednostnima nalogama Komisije, da se Evropo pripravi na digitalno dobo in vzpostavi gospodarstvo, ki bo pripravljeno na prihodnost in bo delovalo za dobrobit ljudi. Sveženj o digitalnih financah vključuje novo strategijo za digitalne finance v finančnem sektorju EU[1], katere cilj je zagotoviti, da bo EU odprtih rok sprejela digitalno revolucijo in jo spodbujala z inovativnimi evropskimi podjetji na čelu, tako da bodo koristi digitalnih financ na voljo potrošnikom in podjetjem. Poleg tega predloga sveženj vključuje tudi predlog uredbe o trgih kriptoimetij[2], predlog uredbe o pilotni ureditvi za tržne infrastrukture na podlagi tehnologije razpršene evidence[3] in predlog direktive za pojasnitev ali spremembo nekaterih povezanih pravil EU o finančnih storitvah[4]. Digitalizacija in operativna odpornost v finančnem sektorju sta dve strani medalje. Digitalne ali informacijske in komunikacijske tehnologije (IKT) ustvarjajo priložnosti, vendar povzročajo tudi tveganja. Ta je treba dobro razumeti in upravljati, zlasti v stresnih razmerah.

Oblikovalci politike in nadzorniki se zato vse bolj osredotočajo na tveganja, ki izhajajo iz zanašanja na IKT. Zlasti so poskušali okrepiti odpornost podjetij z določanjem standardov in usklajevanjem regulativnih ali nadzornih nalog. To delo je bilo izvedeno na mednarodni in evropski ravni v različnih industrijah in za številne posebne sektorje, vključno s finančnimi storitvami.

Vendar tveganja na področju informacijsko-komunikacijske tehnologije še vedno predstavljajo izziv operativni odpornosti, zmogljivosti in stabilnosti finančnega sistema EU. Reforma, ki je sledila finančni krizi leta 2008, je okrepila predvsem finančno odpornost[5] finančnega sektorja EU, pri čemer je tveganja na področju IKT obravnavala le posredno na nekaterih področjih, in sicer v okviru ukrepov za širše obravnavanje operativnih tveganj.

V sklopu sprememb zakonodaje EU o finančnih storitvah, ki so bile izvedene po krizi, so bila vzpostavljena enotna pravila, ki urejajo velik del finančnih tveganj, povezanih s finančnimi storitvami, vendar se digitalna operativna odpornost ni v celoti obravnavala. Ukrepi, sprejeti v zvezi s tem, so imeli veliko značilnosti, ki so omejevale njihovo učinkovitost. Pogosto so bili na primer zasnovani kot direktive za minimalno harmonizacijo ali na načelih temelječe uredbe, kar je omogočalo veliko manevrskega prostora za različne pristope na enotnem trgu. Poleg tega je bila osredotočenost na tveganja na področju IKT v okviru kritja operativnih

---

1 Sporočilo Komisije Evropskemu parlamentu, Evropskemu svetu, Svetu, Evropski centralni banki, Evropskemu ekonomsko-socialnemu odboru in Odboru regij o strategiji EU za digitalne finance, 23. september 2020, COM(2020) 591.

2 Predlog uredbe Evropskega parlamenta in Sveta o trgih kriptoimetij in spremembi Direktive (EU) 2019/1937, COM(2020) 593.

3 Predlog uredbe Evropskega parlamenta in Sveta o pilotni ureditvi za tržne infrastrukture na podlagi tehnologije razpršene evidence, COM(2020) 594.

4 Predlog direktive Evropskega parlamenta in Sveta o spremembi direktiv 2006/43/ES, 2009/65/ES, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 in EU/2016/2341, COM(2020) 596.

5 Različni sprejeti ukrepi so bili v osnovi namenjeni povečanju kapitalskih virov in likvidnosti finančnih subjektov ter zmanjšanju tržnih in kreditnih tveganj.

tveganj omejena ali nepopolna. Nazadnje, ti ukrepi se razlikujejo v sektorski zakonodaji o finančnih storitvah. Zato posredovanje na ravni Unije ni povsem ustrezalo potrebam, ki jih imajo evropski finančni subjekti za upravljanje operativnih tveganj na način, da bi vzdržali učinke incidentov na področju IKT, se odzvali nanje in vnovično vzpostavili delovanje po njih. Prav tako finančnim nadzornikom ni zagotovilo najprimernejših orodij, da bi lahko izpolnjevali svoje mandate za preprečevanje finančne nestabilnosti, ki izhaja iz uresničitve teh tveganj na področju IKT.

Pomanjkanje podrobnih in izčrpnih pravil o digitalni operativni odpornosti na ravni EU je privedlo do vse večjega števila nacionalnih regulativnih pobud (npr. o testiranju digitalne operativne odpornosti) in nadzorniških pristopov (npr. v zvezi z obravnavo odvisnosti od tretjih ponudnikov storitev IKT). Vendar imajo ukrepi na ravni držav članic le omejen učinek glede na čezmejno naravo tveganj na področju IKT. Poleg tega je zaradi neusklajenih nacionalnih pobud prišlo do prekrivanj, nedoslednosti, podvajajočih se zahtev ter visokih upravnih stroškov in stroškov izpolnjevanja obveznosti, zlasti za čezmejne finančne subjekte, ali pa so tveganja na področju IKT ostala neodkrita in zato neobravnavana. Te razmere drobijo enotni trg, slabijo stabilnost in integriteto finančnega sektorja EU ter ogrožajo zaščito potrošnikov in vlagateljev.

Zato je treba vzpostaviti podroben in celovit okvir za digitalno operativno odpornost finančnih subjektov v EU. S tem okvirom se bo poglobila razsežnost enotnih pravil, povezana z upravljanjem digitalnih tveganj. Zlasti se bo okrepilo in racionaliziralo ravnanje finančnih subjektov v zvezi z upravljanjem tveganj na področju IKT, vzpostavilo temeljito testiranje sistemov IKT, povečala ozaveščenost nadzornikov glede kibernetskih tveganj in incidentov, povezanih z IKT, s katerimi se soočajo finančni subjekti, ter uvedla pooblastila za finančne nadzornike za pregled nad tveganji, ki izhajajo iz odvisnosti finančnih subjektov od tretjih ponudnikov storitev IKT. S predlogom se bo vzpostavil dosleden mehanizem poročanja o incidentih, ki bo pomagal zmanjšati upravna bremena za finančne subjekte in okrepil učinkovitost nadzora.

- Skladnost z veljavnimi predpisi s področja zadevne politike

Ta predlog je del širšega prizadevanja na evropski in mednarodni ravni za krepitev kibernetske varnosti na področju finančnih storitev in obravnavanje širših operativnih tveganj[6].

Prav tako odgovarja na skupni tehnični nasvet[7] evropskih nadzornih organov iz leta 2019, v katerem so nadzorni organi pozivali k skladnejšemu pristopu k obravnavi tveganj na področju IKT v finančnem sektorju in Komisiji priporočili, naj sorazmerno okrepi digitalno operativno odpornost industrije finančnih storitev s posebno sektorsko pobudo EU. Nasvet evropskih nadzornih organov je bil odgovor na akcijski načrt za finančno tehnologijo, ki ga je Komisija predstavila leta 2018[8].

- Skladnost z drugimi politikami Unije

---

6 Baselski odbor za finančni nadzor, *Cyber-resilience: Range of practices* (Kibernetska odpornost: različne prakse), december 2018, in *Principles for sound management of operational risk (PSMOR)* (Načela za dobro upravljanje operativnih tveganj), oktober 2014.

7 Skupni nasvet evropskih nadzornih organov Evropski komisiji o potrebi po zakonodajnih izboljšavah v zvezi z zahtevami za upravljanje tveganj na področju IKT v finančnem sektorju EU, JC 2019 26 (2019).

8 Evropska komisija, *Akcijski načrt za finančno tehnologijo*, COM(2018) 109 final.

Kot je v svojih političnih usmeritvah[9] navedla predsednica Ursula von der Leyen in kot je določeno v sporočilu „Oblikovanje digitalne prihodnosti Evrope“[10], je za Evropo ključnega pomena, da v varnih in etičnih okvirih izkoristi vse priložnosti, ki jih nudi digitalna doba, ter okrepi svoje industrijske in inovacijske zmogljivosti. Evropska strategija za podatke[11] določa štiri stebre – varstvo podatkov, temeljne pravice, varnost in kibernetsko varnost –, ki so ključni predpogoji za družbo, ki izkorišča moč podatkov. V zadnjem času Evropski parlament pripravlja poročilo o digitalnih financah, ki med drugim poziva k skupnemu pristopu h kibernetski odpornosti finančnega sektorja[12]. Zakonodajni okvir, ki krepi digitalno operativno odpornost finančnih subjektov EU, je skladen s temi cilji politike. Predlog bi podprl tudi politike, namenjene okrevanju po učinkih koronavirusa, saj bi zagotovil, da je večje zanašanje na digitalne finance tesno povezano z operativno odpornostjo.

Pobuda bi ohranila koristi, povezane s horizontalnim okvirom kibernetske varnosti (npr. direktivo o varnosti omrežij in informacij oziroma direktivo o kibernetski varnosti (NIS)), tako da bi finančni sektor še naprej ostal na njenem področju uporabe. Finančni sektor bi ostal tesno povezan z organom za sodelovanje na področju varnosti omrežij in informacij, finančni nadzorniki pa bi si lahko izmenjali ustrezne informacije v obstoječem ekosistemu NIS. Pobuda bi bila skladna 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. Nazadnje je ta predlog popolnoma v skladu s strategijo za varnostno unijo[13], ki je pozvala k pobudi o digitalni operativni odpornosti finančnega sektorja, saj je ta zelo odvisen od storitev IKT in zelo izpostavljen kibernetskim napadom.

2. PRAVNA PODLAGA, SUBSIDIARNOST IN SORAZMERNOST

- Pravna podlaga

Predlog uredbe temelji na členu 114 PDEU.

Odpravlja ovire za vzpostavitev in delovanje notranjega trga za finančne storitve ter ju krepi s harmonizacijo pravil, ki se uporabljajo pri upravljanju tveganj na področju IKT, poročanju, testiranju in tveganjih tretjih oseb na področju IKT. Trenutne razlike na tem področju, tako na zakonodajni in nadzorni ravni kot tudi na državni ravni in ravni EU, ovirajo enotni trg za finančne storitve, ker se finančni subjekti, ki se ukvarjajo s čezmejnimi dejavnostmi, soočajo z različnimi, če ne celo prekrivajočimi se regulativnimi zahtevami ali pričakovanji glede nadzora, ki bi lahko ovirala uveljavljanje njihove pravice do ustanavljanja in opravljanja storitev. Različna pravila tudi izkrivljajo konkurenco med finančnimi subjekti iste vrste v različnih državah članicah. Poleg tega lahko oblikovanje različnih nacionalnih pravil ali pristopov, ki že veljajo ali so v postopku sprejetja in izvajanja na nacionalni ravni, na področjih, kjer harmonizacije ni oziroma je delna ali omejena, odvrača od svobode

---

9 Predsednica Ursula Von Der Leyen, Politične usmeritve naslednje Evropske komisije za obdobje 2019–2024, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_sl.pdf.

10 Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, *Oblikovanje digitalne prihodnosti Evrope*, COM(2020) 67 final.

11 Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, *Evropska strategija za podatke*, COM(2020) 66 final.

12 Poročilo s priporočili Komisiji o digitalnih finančnih storitvah: nova tveganja pri kriptosredstvih – regulativni in nadzorni izzivi na področju finančnih storitev, institucij in trgov (2020/2034(INL)), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=en.

13 Sporočilo Komisije Evropskemu parlamentu, Evropskemu svetu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij o strategiji EU za varnostno unijo, COM(2020) 605 final.

opravljanja finančnih storitev na enotnem trgu. To zlasti velja za okvire digitalnega operativnega testiranja in nadzor nad ključnimi tretjimi ponudniki storitev IKT.

Ker predlog vpliva na več direktiv Evropskega parlamenta in Sveta, ki so bile sprejete na podlagi člena 53(1) PDEU, se hkrati sprejme tudi predlog direktive, ki odraža potrebne spremembe teh direktiv.

- Subsidiarnost

Zaradi visoke stopnje medsebojne povezanosti finančnih storitev, znatne čezmejne dejavnosti finančnih subjektov in velike odvisnosti celotnega finančnega sektorja od tretjih ponudnikov storitev IKT je z vidika skupnega interesa za ohranitev trdnosti finančnih trgov EU potrebna močna digitalna operativna odpornost. Razlike, ki so posledica neenakomernih ali delno harmoniziranih ureditev, prekrivanj ali več zahtev, ki veljajo za iste finančne subjekte, ki poslujejo čezmejno ali imajo več dovoljenj[14] na enotnem trgu, je mogoče učinkovito reševati le na ravni Unije.

S tem predlogom se usklajuje digitalna operativna komponenta globoko integriranega in medsebojno povezanega sektorja, ki že ima koristi od enotnega sklopa pravil in nadzora na večini drugih ključnih področij. V zadevah, kot je poročanje o incidentih, povezanih z IKT, bi lahko le harmonizirana pravila Unije zmanjšala upravna bremena in znižala finančne stroške, povezane s poročanjem o istem incidentu, povezanem z IKT, različnim organom Unije in nacionalnim organom. Ukrepi EU so potrebni tudi, da se omogoči vzajemno priznavanje rezultatov naprednega testiranja digitalne operativne odpornosti za subjekte, ki poslujejo čezmejno in za katere zaradi neobstoja pravil Unije veljajo ali bi lahko veljali različni okviri v različnih državah članicah. Samo ukrepanje na ravni Unije lahko odpravi razlike v načinih testiranja, ki so jih uvedle države članice. Potrebno je tudi za obravnavo pomanjkanja ustreznih nadzornih pooblastil za spremljanje tveganj, ki izhajajo iz tretjih ponudnikov storitev IKT, vključno s tveganji koncentracije in medsebojnih negativnih vplivov za finančni sektor EU.

- Sorazmernost

Predlagana pravila ne presegajo okvirov, ki so potrebni za dosego ciljev predloga. Zajemajo samo vidike, ki jih države članice ne morejo doseči same in pri katerih so upravno breme in stroški sorazmerni s posebnimi in splošnimi cilji, ki jih je treba doseči.

Sorazmernost je zasnovana glede na obseg in intenzivnost z uporabo kvalitativnih in kvantitativnih meril ocenjevanja. Namen teh meril je zagotoviti, da nova pravila zajemajo vse finančne subjekte, vendar so hkrati prilagojena tveganjem in potrebam njihovih posebnih značilnosti v smislu njihove velikosti in poslovnih profilov. Sorazmernost je vključena tudi v pravila o upravljanju tveganj na področju IKT, testiranju digitalne odpornosti, poročanju o večjih incidentih, povezanih z IKT, in nadzoru nad ključnimi tretjimi ponudniki storitev IKT.

- Izbira instrumenta

Ukrepi, potrebni za urejanje upravljanja tveganj na področju IKT, poročanja o incidentih, povezanih z IKT, testiranja in nadzora nad ključnimi tretjimi ponudniki storitev IKT, morajo biti vključeni v Uredbo, da se zagotovi enotna učinkovita in neposredna uporaba podrobnih

[14] Isti finančni subjekt ima lahko dovoljenje za bančništvo, investicijsko podjetje in plačilno institucijo, pri čemer vsako dovoljenje izda drug nadzornik v eni ali več državah članicah.

zahtev, brez poseganja v sorazmernost in posebna pravila, predvidena s to uredbo. Doslednost pri obravnavanju digitalnih operativnih tveganj prispeva h krepitvi zaupanja v finančni sistem in ohranja njegovo stabilnost. Ker uporaba uredbe pomaga zmanjšati regulativno zapletenost, spodbuja konvergenco nadzora in krepi pravno varnost, ta uredba prispeva tudi k omejevanju stroškov finančnih subjektov za izpolnjevanje obveznosti, zlasti za tiste subjekte, ki poslujejo čezmejno, kar bi pripomoglo k odpravi izkrivljanja konkurence.

Ta uredba odpravlja tudi zakonodajne razlike in neenakomerne nacionalne regulativne ali nadzorne pristope k tveganjem na področju IKT in tako odpravlja ovire za enotni trg za finančne storitve, zlasti za nemoteno uveljavljanje pravice do ustanavljanja in opravljanja storitev pri finančnih subjektih, ki delujejo čezmejno.

Nazadnje, enotna pravila so bila večinoma oblikovana na podlagi uredb, njihova posodobitev s komponento digitalne operativne odpornosti pa bi morala slediti isti izbiri pravnega instrumenta.

3. REZULTATI NAKNADNIH OCEN, POSVETOVANJ Z ZAINTERESIRANIMI STRANMI IN OCEN UČINKA

- Naknadne ocene/preverjanja ustreznosti obstoječe zakonodaje

Do zdaj se nobena zakonodaja Unije o finančnih storitvah ni osredotočala na operativno odpornost ali se celovito lotila tveganj, ki izhajajo iz digitalizacije, niti tiste ne, katerih pravila obravnavajo razsežnost operativnega tveganja na splošno in tveganja na področju IKT kot njegovo podkomponento. Unija je z dosedanjim posredovanjem pomagala obravnavati potrebe in težave, ki so se pojavile po finančni krizi leta 2008: kreditne institucije niso bile dovolj kapitalizirane, finančni trgi niso bili dovolj integrirani, harmonizacija do takrat pa je bila minimalna. Tveganje na področju IKT se takrat ni štelo za prednostno nalogo, zato so se pravni okviri za različne finančne podsektorje razvijali neusklajeno. Kljub temu so ukrepi Unije dosegli cilje zagotavljanja finančne stabilnosti in vzpostavitve enotnega sklopa harmoniziranih bonitetnih pravil in pravil ravnanja na trgu, ki veljajo za finančne subjekte po vsej EU. Ker dejavniki, ki so v preteklosti vplivali na zakonodajno posredovanje Unije, niso omogočali posebnih ali celovitih pravil za obravnavanje široke uporabe digitalnih tehnologij in posledičnih finančnih tveganj, se zdi eksplicitno vrednotenje težavno. Implicitno vrednotenje in posledične zakonodajne spremembe se izražajo v vseh stebrih te uredbe.

- Posvetovanja z zainteresiranimi stranmi

Komisija se je med postopkom priprave tega predloga posvetovala z zainteresiranimi stranmi, zlasti:

(i) Komisija je izvedla namensko odprto javno posvetovanje (19. december 2019 – 19. marec 2020)[15];

(ii) Komisija se je posvetovala z javnostjo na podlagi začetne ocene učinka (19. december 2019 – 16. januar 2020)[16];

[15] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation.

[16] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-.

(iii) službe Komisije so se dvakrat posvetovale s strokovnjaki držav članic v strokovni skupini za bančništvo, plačila in zavarovanje (EGBPI) (18. maja 2020 in 16. julija 2020)[17];

(iv) službe Komisije so izvedle namenski spletni seminar o digitalni operativni odpornosti v okviru javnih predstavitev in razprav o digitalnih financah v letu 2020 (19. maja 2020).

Namen javnega posvetovanja je bil Komisijo obvestiti o razvoju potencialnega medsektorskega okvira EU za digitalno operativno odpornost na področju finančnih storitev. Odzivi so pokazali široko podporo uvedbi namenskega okvira z ukrepi, osredotočenimi na štiri področja, ki so bila predmet posvetovanja, pri čemer je bila poudarjena potreba po zagotavljanju sorazmernosti ter skrbni obravnavi in razlagi medsebojnega delovanja s horizontalnimi pravili direktive o kibernetski varnosti. Komisija je prejela dva odgovora na začetno oceno učinka, v katerih so anketiranci obravnavali posebne vidike, povezane z njihovim področjem dejavnosti.

Države članice so na srečanju skupine EGBPI, ki je potekalo 18. maja 2020, izrazile močno podporo krepitvi digitalne operativne odpornosti finančnega sektorja z ukrepi, predvidenimi v okviru štirih elementov, ki jih je opisala Komisija. Prav tako so države članice poudarile potrebo po jasni uskladitvi novih pravil s pravili o operativnem tveganju (v okviru zakonodaje EU o finančnih storitvah) in s horizontalnimi pravili o kibernetski varnosti (direktiva NIS). Na drugem srečanju so nekatere države članice poudarile, da je treba zagotoviti sorazmernost in upoštevati poseben položaj majhnih podjetij ali odvisnih družb večjih skupin ter poskrbeti za trdna pooblastila nacionalnih organov, ki sodelujejo pri nadzoru.

Predlog se opira tudi na povratne informacije, pridobljene na srečanjih z zainteresiranimi stranmi ter organi in institucijami EU, in jih upošteva. Zainteresirane strani, vključno s tretjimi ponudniki storitev IKT, so izrazile splošno podporo. Analiza prejetih povratnih informacij kaže na željo, da se pri oblikovanju pravil ohrani sorazmernost ter upošteva pristop, ki temelji na načelih in tveganju. Na institucionalni strani so glavna mnenja podali Evropski odbor za sistemska tveganja (ESRB), evropski nadzorni organi, Agencija Evropske unije za kibernetsko varnost (ENISA) in Evropska centralna banka (ECB) ter pristojni organi držav članic.

- Zbiranje in uporaba strokovnih mnenj

Pri pripravi tega predloga se je Komisija opirala na kvalitativne in kvantitativne dokaze, zbrane iz priznanih virov, vključno z dvema skupnima tehničnima nasvetoma evropskih nadzornih organov. To je bilo dopolnjeno z zaupnimi mnenji in javno dostopnimi poročili nadzornih organov, mednarodnih organov za določanje standardov in vodilnih raziskovalnih inštitutov ter kvantitativnimi in kvalitativnimi prispevki opredeljenih zainteresiranih strani v svetovnem finančnem sektorju.

- Ocena učinka

Temu predlogu je priložena ocena učinka[18], ki je bila 29. aprila 2020 predložena Odboru za regulativni nadzor in odobrena 29. maja 2020. Odbor za regulativni nadzor je predlagal

[17] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/expert-group-banking-payments-and-insurance_sl.

izboljšave na nekaterih področjih za: (i) zagotovitev več informacij o tem, kako bi se zagotovila sorazmernost; (ii) natančnejšo opredelitev, koliko se prednostna možnost razlikuje od skupnih tehničnih nasvetov evropskih nadzornih organov in zakaj je ta možnost optimalna, in (iii) nadaljnjo opredelitev, kako predlog deluje skupaj z obstoječo zakonodajo EU, vključno s pravili, ki se trenutno pregledujejo. Ocena učinka je bila spremenjena tako, da obravnava te točke in podrobnejše pripombe Odbora za regulativni nadzor.

Komisija je preučila številne možnosti politike za razvoj okvira za digitalno operativno odpornost:

- „brez ukrepanja“: sedanje različne določbe EU o finančnih storitvah, deloma tudi direktiva o kibernetski varnosti, in obstoječe ali prihodnje nacionalne ureditve bi še naprej določale pravila o operativni odpornosti;
- možnost 1: krepitev kapitalskih blažilnikov: uvedli bi se dodatni kapitalski blažilniki za povečanje zmožnosti finančnih subjektov, da pokrijejo izgube, ki bi lahko nastale zaradi neobstoja digitalne operativne odpornosti;
- možnost 2: uvedba akta o digitalni operativni odpornosti na področju finančnih storitev: uvedba celovitega okvira na ravni EU z doslednimi pravili, ki obravnavajo potrebe po digitalni operativni odpornosti vseh reguliranih finančnih subjektov, in vzpostavitev okvira nadzora za ključne tretje ponudnike storitev IKT;
- možnost 3: akt o digitalni operativni odpornosti na področju finančnih storitev v kombinaciji s centraliziranim nadzorom ključnih tretjih ponudnikov storitev IKT: poleg uvedbe akta o digitalni operativni odpornosti (možnost 2) bi bil ustanovljen nov organ za nadzor nad opravljanjem storitev, ki jih zagotavljajo tretji ponudniki storitev IKT.

Izbrana je bila druga možnost, saj večino predvidenih ciljev dosega na način, ki je učinkovit, uspešen in skladen z drugimi politikami Unije. Tudi večina zainteresiranih strani je podprla to možnost.

Izbrana možnost bi privedla do enkratnih in ponavljajočih se stroškov[19]. Enkratni stroški so v glavnem posledica naložb v informacijske sisteme in jih je težko količinsko opredeliti glede na različna stanja zapletenih informacijskih okolij podjetij in zlasti njihovih obstoječih informacijskih sistemov. Kljub temu bodo ti stroški za velika podjetja verjetno omejeni, saj so ta že izvedla znatne naložbe v informacijsko-komunikacijske tehnologije. Stroški naj bi bili omejeni tudi za manjša podjetja, saj bi glede na njihovo manjše tveganje veljali sorazmerni ukrepi.

Izbrana možnost bi imela pozitiven gospodarski, socialni in okoljski učinek na mala in srednja podjetja, ki poslujejo v sektorju finančnih storitev. Predlog bo malim in srednjim podjetjem zagotovil jasnost v zvezi s tem, katera pravila veljajo, kar bo znižalo stroške izpolnjevanja obveznosti.

---

[18] Delovni dokument služb Komisije – Poročilo o oceni učinka, ki spremlja dokument 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, SWD(2020) 198 z dne 24. septembra 2020.

[19] Prav tam, str. 89–94.

Glavni socialni učinki izbrane možnosti politike bi bili na potrošnike in vlagatelje. Višja stopnja digitalne operativne odpornosti finančnega sistema EU bi zmanjšala število incidentov in znižala njihove povprečne stroške. Celotna družba bi imela koristi od povečanega zaupanja v sektor finančnih storitev.

Nazadnje, z vidika vpliva na okolje bi izbrana možnost politike spodbudila širšo uporabo najnovejše generacije infrastruktur in storitev IKT, ki naj bi postale okoljsko bolj trajnostne.

- Ustreznost in poenostavitev ureditve

Odprava prekrivajočih se zahtev glede poročanja o incidentu, povezanem z IKT, bi zmanjšala upravna bremena in znižala povezane stroške. Poleg tega se bodo s harmoniziranim testiranjem digitalne operativne odpornosti, vzajemno priznanim na enotnem trgu, znižali stroški, zlasti za čezmejna podjetja, ki bi morala sicer morda izvesti več testiranj v različnih državah članicah[20].

- Temeljne pravice

EU je zavezana zagotavljanju visokih standardov varstva temeljnih pravic. Vsi dogovori o prostovoljni izmenjavi informacij med finančnimi subjekti, ki jih spodbuja ta uredba, bi se izvajali v zaupanja vrednih okoljih ob popolnem spoštovanju pravil Unije o varstvu podatkov, predvsem Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta[21], zlasti kadar je obdelava osebnih podatkov potrebna za namene zakonitega interesa, za katerega si prizadeva upravljavec.

4. PRORAČUNSKE POSLEDICE

Ker sedanja uredba predvideva okrepljeno vlogo evropskih nadzornih organov s pooblastili, ki so jim dodeljena za ustrezen nadzor nad ključnimi tretjimi ponudniki storitev IKT, bi predlog v smislu proračunskih posledic povzročil povečanje sredstev, zlasti za izpolnjevanje nadzornih nalog (kot so inšpekcijski pregledi in revizije na kraju samem in na spletu) ter uporabo osebja s specifičnim strokovnim znanjem na področju varnosti IKT.

Obseg in porazdelitev teh stroškov bosta odvisna od obsega novih nadzornih pooblastil in (natančnih) nalog, ki jih bodo izvajali evropski nadzorni organi. Kar zadeva zagotavljanje novih kadrovskih virov, bodo EBA, ESMA in EIOPA skupaj potrebovali 18 redno zaposlenih s polnim delovnim časom (EPDČ), in sicer vsak po šest EPDČ, ko bodo začele veljati različne določbe predloga (ocenjeno na 15,71 milijona EUR za obdobje 2022–2027). Tudi evropski nadzorni organi bodo imeli dodatne stroške za informacijsko tehnologijo, stroške službenih potovanj za inšpekcijske preglede na kraju samem in stroške prevajanja (ocenjene na 12 milijonov EUR za obdobje 2022–2027) ter druge upravne odhodke (ocenjene na 2,48 milijona EUR za obdobje 2022–2027). Zato predvideni skupni stroški znašajo približno 30,19 milijona EUR za obdobje 2022–2027.

Upoštevati je treba tudi, da bo število zaposlenih (npr. novi člani osebja in drugi odhodki, povezani z novimi nalogami), ki so potrebni za neposredni nadzor, sčasoma odvisno od spreminjanja števila in velikosti ključnih tretjih ponudnikov storitev IKT, ki bodo pod nadzorom, vendar se bodo ustrezni odhodki v celoti financirali z nadomestili, ki jih bodo

[20] Prav tam.

[21] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

plačevali navedeni udeleženci na trgu. Zato vpliv na odobrena proračunska sredstva EU ni predviden (razen za dodatne člane osebja), saj se bodo ti stroški v celoti financirali z nadomestili.

Finančni in proračunski učinki tega predloga so podrobno pojasnjeni v oceni finančnih posledic zakonodajnega predloga, ki je priložena temu predlogu.

5. DRUGI ELEMENTI

- Načrti za izvedbo ter ureditev spremljanja, ocenjevanja in poročanja

Predlog vključuje splošni načrt za spremljanje in ocenjevanje učinka na specifične cilje, pri čemer se zahteva, da Komisija opravi pregled vsaj tri leta po začetku veljavnosti in o svojih glavnih ugotovitvah poroča Evropskemu parlamentu in Svetu.

Pregled je treba izvesti v skladu s smernicami Komisije za boljše pravno urejanje.

- Natančnejša pojasnitev posameznih določb predloga

Predlog temelji na več glavnih področjih politike, ki so ključni medsebojno povezani stebri, sporazumno vključeni v evropske in mednarodne smernice ter dobre prakse za povečanje kibernetske in operativne odpornosti finančnega sektorja.

Področje uporabe Uredbe in sorazmerna uporaba zahtevanih ukrepov (člen 2)

Da bi se zagotovila doslednost glede zahtev za upravljanje tveganj na področju IKT, ki veljajo za finančni sektor, Uredba zajema vrsto finančnih subjektov, reguliranih na ravni Unije, in sicer kreditne institucije, plačilne institucije, institucije za izdajo elektronskega denarja, investicijska podjetja, ponudnike storitev v zvezi s kriptoimetji, centralne depotne družbe, centralne nasprotne stranke, mesta trgovanja, repozitorije sklenjenih poslov, upravitelje alternativnih investicijskih skladov in družbe za upravljanje, izvajalce storitev sporočanja podatkov, zavarovalnice in pozavarovalnice, zavarovalne posrednike, pozavarovalne posrednike in posrednike dopolnilnih zavarovanj, institucije za poklicno pokojninsko zavarovanje, bonitetne agencije, zakonite revizorje in revizijska podjetja, upravljavce ključnih referenčnih vrednosti in ponudnike storitev množičnega financiranja.

Taka pokritost omogoča homogeno in skladno uporabo vseh komponent upravljanja tveganj na področjih, povezanih z IKT, ter zagotavlja enake konkurenčne pogoje med finančnimi subjekti glede njihovih regulativnih obveznosti v zvezi s tveganji na področju IKT. Hkrati se v Uredbi priznava, da obstajajo pomembne razlike med finančnimi subjekti v smislu velikosti, poslovnih profilov ali glede na njihovo izpostavljenost digitalnemu tveganju. Ker imajo večji finančni subjekti več virov, morajo samo finančni subjekti, ki niso mikro podjetja, na primer vzpostaviti zapletene ureditve upravljanja, namenske funkcije upravljanja, izvajati poglobljene ocene po večjih spremembah infrastrukture omrežja in informacijskega sistema, redno izvajati analize tveganj za obstoječe sisteme IKT, razširiti testiranje neprekinjenega poslovanja ter načrtov odzivanja in okrevanja po katastrofi, da bi zajeli scenarije preklopa med primarno infrastrukturo IKT in redundantnimi obrati. Poleg tega bodo morali penetracijsko testiranje na podlagi analize groženj izvajati le finančni subjekti, ki so bili opredeljeni kot pomembni za namene naprednega testiranja digitalne odpornosti.

Pokritost je široka, vendar ni izčrpna. Ta uredba ne zajema upravljavcev sistema, kot so opredeljeni v točki (p) člena 2 Direktive 98/26/ES[22] o dokončnosti poravnave pri plačilih in sistemih poravnave vrednostnih papirjev, in udeležencev v sistemu, razen če je tak udeleženec tudi sam finančni subjekt, reguliran na ravni Unije in bi zato zanj veljala ta uredba (tj. kreditna institucija, investicijsko podjetje, centralna nasprotna stranka). Prav tako na to področje uporabe ne spada register Unije za pravice do emisije, ki se v skladu z Direktivo 2003/87/ES[23] upravlja pod okriljem Evropske komisije.

Pri takih izključitvah iz direktive o dokončnosti poravnave se upošteva potreba po nadaljnji reviziji pravnih in političnih zadev, ki se nanašajo na upravljavce in udeležence sistemov o dokončnosti poravnave, ob ustreznem upoštevanju učinka okvirov, ki trenutno veljajo za plačilne sisteme[24], ki jih upravljajo centralne banke. Ker lahko te zadeve vključujejo vidike, ki se še vedno razlikujejo od vprašanj, zajetih v tej uredbi, bo Komisija še naprej ocenjevala nujnost in učinek nadaljnje razširitve področja uporabe te uredbe na subjekte in infrastrukture IKT, ki so trenutno zunaj njene pristojnosti.

Zahteve, povezane z upravljanjem (člen 4)

Ta uredba je namenjena boljši uskladitvi poslovnih strategij finančnih subjektov in izvajanju upravljanja tveganj na področju IKT. V ta namen bo moral upravljalni organ ohraniti ključno aktivno vlogo pri usmerjanju okvira za upravljanje tveganj na področju IKT in si prizadevati za spoštovanje stroge kibernetske higiene. Polna odgovornost upravljalnega organa pri upravljanju tveganj finančnega subjekta na področju IKT bo poglavitno načelo, ki se bo nadalje preneslo v sklop posebnih zahtev, kot so dodelitev jasnih vlog in odgovornosti za vse funkcije, povezane z IKT, stalno sodelovanje pri nadzoru spremljanja upravljanja tveganj na področju IKT, pa tudi pri celotnem sklopu postopkov odobritve in nadzora ter ustrezni dodelitvi naložb in usposabljanj na področju IKT.

Zahteve, povezane z upravljanjem tveganj na področju IKT (členi 5 do 14)

Digitalna operativna odpornost temelji na nizu ključnih načel in zahtev glede upravljanja tveganj na področju IKT v skladu s skupnim tehničnim nasvetom evropskih nadzornih organov. Te zahteve, ki temeljijo na ustreznih mednarodnih, nacionalnih in sektorskih standardih, smernicah in priporočilih, se nanašajo na posebne funkcije pri upravljanju tveganj na področju IKT (identifikacija, zaščita in preprečevanje, odkrivanje, odzivanje in okrevanje, učenje in razvoj ter komunikacija). Da bi finančni subjekti lahko sledili hitro razvijajočemu se področju kibernetskih groženj, morajo vzpostaviti in vzdrževati odporne sisteme in orodja IKT, ki zmanjšujejo učinek tveganj na področju IKT, stalno prepoznavati vse vire tveganj na področju IKT, vzpostaviti zaščitne in preventivne ukrepe, sproti odkrivati neobičajne dejavnosti, vzpostaviti namenske in celovite politike neprekinjenega poslovanja ter načrte okrevanja po katastrofi kot sestavni del politike neprekinjenega poslovanja. Zadnje navedene komponente so potrebne za takojšnjo okrevanje po katastrofi po incidentih, povezanih z IKT, zlasti kibernetskih napadov, z omejevanjem škode in dajanjem prednosti varnemu nadaljevanju dejavnosti. Uredba sama po sebi ne uvaja posebne standardizacije, temveč

[22] Direktiva 98/26/ES Evropskega parlamenta in Sveta z dne 19. maja 1998 o dokončnosti poravnave pri plačilih in sistemih poravnave vrednostnih papirjev (UL L 166, 11.6.1998, str. 45).

[23] Direktiva 2003/87/ES Evropskega parlamenta in Sveta z dne 13. oktobra 2003 o vzpostavitvi sistema za trgovanje s pravicami do emisije toplogrednih plinov v Skupnosti in o spremembi Direktive Sveta 96/61/ES (UL L 275, 25.10.2003, str. 32).

[24] Zlasti Uredba Evropske centralne banke (EU) št. 795/2014 z dne 3. julija 2014 o pregledniških zahtevah za sistemsko pomembne plačilne sisteme.

temelji na evropskih in mednarodno priznanih tehničnih standardih ali dobrih praksah v panogi, če so v celoti v skladu z nadzorniškimi navodili o uporabi in vključitvi takih mednarodnih standardov. Ta uredba zajema tudi celovitost, varnost in odpornost fizične infrastrukture in objektov, ki podpirajo uporabo tehnologije, ter ustreznih postopkov in ljudi, povezanih z IKT, v okviru digitalnega odtisa poslovanja finančnega subjekta.

Poročanje o incidentih, povezanih z IKT (členi 15 do 20)

Harmonizacija in racionalizacija poročanja o incidentih, povezanih z IKT, se doseže najprej s splošno zahtevo, da finančni subjekti vzpostavijo in izvajajo postopek upravljanja za spremljanje in evidentiranje incidentov, povezanih z IKT, čemur sledi obveznost, da jih razvrstijo na podlagi meril, ki so podrobno opisana v Uredbi in so jih nadalje razvili evropski nadzorni organi ter s katerimi se opredelijo pragi pomembnosti. Drugič, pristojnim organom je treba poročati samo o večjih incidentih, povezanih z IKT. Poročanje poteka i z uporabo skupne predloge in po harmoniziranem postopku, ki ga razvijejo evropski nadzorni organi. Finančni subjekti bi morali predložiti začetna, vmesna in končna poročila ter obvestiti svoje uporabnike in stranke, če incident vpliva ali bi lahko vplival na njihove finančne interese. Pristojni organi bi morali posredovati ustrezne podrobnosti o incidentih drugim institucijam ali organom: evropskim nadzornim organom, Evropski centralni banki in enotnim kontaktnim točkam, določenim v skladu z Direktivo (EU) 2016/1148.

Za začetek dialoga med finančnimi subjekti in pristojnimi organi, ki bi pomagal zmanjšati učinek na najmanjšo možno mero in določiti ustrezne popravne ukrepe, bi bilo treba poročanje o večjih incidentih, povezanih z IKT, dopolniti s povratnimi informacijami in smernicami nadzornikov.

Nazadnje, možnost centralizacije poročanja o incidentih, povezanih z IKT, na ravni Unije bi bilo treba nadalje preučiti v skupnem poročilu evropskih nadzornih organov, Evropske centralne banke in ENISA, v katerem bi se ocenjevala izvedljivost vzpostavitve enotnega vozlišča EU, kjer bi lahko finančni subjekti poročali o večjih incidentih, povezanih z IKT.

Testiranje digitalne operativne odpornosti (členi 21 do 24)

Zmogljivosti in funkcije, vključene v okvir upravljanja tveganj na področju IKT, je treba redno testirati v smislu pripravljenosti in prepoznavanja slabosti, pomanjkljivosti ali vrzeli ter takojšnjega izvajanja popravnih ukrepov. Ta uredba omogoča sorazmerno uporabo zahtev za testiranje digitalne operativne odpornosti glede na velikost, poslovanje in profile tveganj finančnih subjektov: vsi subjekti bi morali testirati sisteme in orodja IKT, vendar bi bilo treba napredno penetracijsko testiranje na podlagi analize groženj zahtevati le od tistih subjektov, ki so jih pristojni organi (na podlagi meril, ki so določena v tej uredbi in jih nadalje oblikujejo evropski nadzorni organi) opredelili kot pomembne in kibernetsko pripravljene. Ta uredba določa tudi zahteve za preskuševalce in priznavanje rezultatov penetracijskega testiranja na podlagi analize groženj po vsej Uniji za finančne subjekte, ki delujejo v več državah članicah.

Tveganja tretjih oseb na področju IKT (členi 25 do 39)

Uredba je zasnovana tako, da zagotavlja dobro spremljanje tveganj tretjih oseb na področju IKT. Ta cilj bo dosežen, prvič, s spoštovanjem na načelih temelječih pravil, ki veljajo za spremljanje tveganj, povezanih s tretjimi ponudniki storitev IKT, ki ga izvajajo finančni subjekti. Drugič, ta uredba usklajuje ključne elemente storitev tretjih ponudnikov storitev IKT in odnosa z njimi. Ti elementi zajemajo minimalne vidike, ki se štejejo za bistvene, da lahko finančni subjekt v celoti spremlja tveganja tretje osebe na področju IKT v vseh fazah sklenitve, izvajanja in prenehanja pogodbe ter v vseh popogodbenih fazah njunega odnosa.

Predvsem bodo pogodbe, ki urejajo ta odnos, morale vsebovati popoln opis storitev, navedbo lokacij, kjer se bodo podatki obdelali, celovite opise ravni storitev, ki jih spremljajo

kvantitativni in kvalitativni cilji uspešnosti, ustrezne določbe o dostopnosti, razpoložljivosti, celovitosti, varnosti in zaščiti osebnih podatkov ter jamstva glede dostopa, okrevanja in povračil v primeru prenehanja delovanja tretjih ponudnikov storitev IKT, odpovedne roke in obveznosti poročanja tretjih ponudnikov storitev IKT, pravice do dostopa, inšpekcijskih pregledov in revizij s strani finančnega subjekta ali imenovane tretje osebe, jasne pravice do odpovedi in namenske izhodne strategije. Ker je mogoče nekatere od teh pogodbenih elementov standardizirati, Uredba spodbuja prostovoljno uporabo standardnih pogodbenih klavzul, ki jih bo Komisija pripravila za uporabo storitve računalništva v oblaku.

Nazadnje, Uredba poskuša spodbuditi konvergenco nadzornih pristopov k tveganjem tretjih oseb na področju IKT v finančnem sektorju, tako da vzpostavlja okvir nadzora Unije za ključne tretje ponudnike storitev IKT. Z novim harmoniziranim zakonodajnim okvirom bo evropski nadzorni organ, ki bo imenovan za glavnega nadzornika za vsakega takega ključnega tretjega ponudnika storitev IKT, prejel pooblastila za zagotavljanje, da se ponudniki tehnoloških storitev, ki imajo ključno vlogo pri delovanju finančnega sektorja, ustrezno spremljajo na vseevropski ravni. Okvir nadzora, ki ga predvideva ta uredba, temelji na obstoječi institucionalni arhitekturi na področju finančnih storitev, pri čemer Skupni odbor evropskih nadzornih organov zagotavlja medsektorsko usklajevanje v zvezi z vsemi zadevami o tveganju na področju IKT v skladu s svojimi nalogami na področju kibernetske varnosti, pri čemer ga pri tem podpira pododbor (nadzorniški forum), ki izvaja pripravljalno delo za posamezne odločitve in skupna priporočila za ključne tretje ponudnike storitev.

Izmenjava informacij (člen 40)

Da bi se povečala ozaveščenost o tveganjih na področju IKT, na najmanjšo možno mero zmanjšalo njihovo širjenje ter podprle obrambne zmožnosti in tehnike finančnih subjektov za odkrivanje groženj, Uredba finančnim subjektom omogoča, da sklenejo dogovore za medsebojno izmenjavo informacij in obveščevalnih podatkov o kibernetskih grožnjah.

2020/0266 (COD)

Predlog

UREDBA 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[25],

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora[26],

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. 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, sklepanje zavarovanj, obravnavo zahtevkov in operacije zalednih služb. 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[27], ponovno potrdil, da lahko obstoječa visoka stopnja

[25] [*dodati sklic*] UL C , , str. .

[26] [*dodati sklic*] UL C , , str. .

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 v Uniji[28] 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.

(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 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[29] 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

---

27 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.

28 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.

29 Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropski centralni banki, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, *Akcijski načrt za finančno tehnologijo: za bolj konkurenčen in inovativen evropski finančni sektor*, COM(2018) 109 final, https://ec.europa.eu/info/publications/180308-action-plan-fintech_sl.

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, ki so odgovorni za spremljanje in varstvo finančne stabilnosti in celovitosti trga.

(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 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.

(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.

(13) Finančni subjekti bi morali pri obravnavanju tveganj na področju IKT slediti istemu pristopu in upoštevati ista na načelih temelječa pravila. Doslednost prispeva k povečanju zaupanja v finančni sistem in ohranjanju njegove stabilnosti, zlasti v primerih prekomerne uporabe 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.

(15) Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta[30] 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

[30] 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).

storitvah, zato je tudi harmonizacija večja v primerjavi z zahtevami iz Direktive (EU) 2016/1148. Posledično je ta uredba *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 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. 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.

(18) Prav tako je pomembno zagotoviti skladnost z direktivo o evropski kritični infrastrukturi[31], ki se trenutno pregleduje, da bi se povečali zaščita in odpornost kritične infrastrukture proti grožnjam, ki niso povezane s kibernetsko varnostjo, 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. 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 na področju IKT. Raven digitalne operativne odpornosti finančnega sistema je treba dvigniti ter hkrati omogočiti sorazmerno

[31] 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).

uporabo zahtev za finančne subjekte, ki so mikro podjetja, kot so opredeljena v Priporočilu Komisije 2003/361/ES[32].

(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)[33] 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.

(22) Določiti je treba pravila za dopolnitev ureditve poročanja o incidentih, povezanih z IKT, z zahtevami, ki trenutno manjkajo v zakonodaji finančnega podsektorja, ter odpravo 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. 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 neusklajenih nacionalnih okvirih, ki ista vprašanja obravnavajo na različne načine. To vodi do podvajanja stroškov za čezmejne finančne subjekte in otežuje 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 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

---

[32] Priporočilo Komisije z dne 6. maja 2003 o opredelitvi mikro, malih in srednje velikih podjetij (UL L 124, 20.5.2003, str. 36).

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

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[34], 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 omogočali kakovostno in količinsko opredelitev ter odpravo posledic tveganj na

[34] 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).

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 so ključni ponudniki za finančne subjekte.

(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.

(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.

(32) Finančne subjekte bi bilo zato treba 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[35] in na način, ki zagotavlja popolno spoštovanje pravil Unije o varstvu podatkov, zlasti Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta[36], predvsem kadar je obdelava osebnih podatkov potrebna za namene zakonitega 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 morala uporaba pravil o digitalni operativni odpornosti upoštevati pomembne razlike med finančnimi subjekti glede njihove velikosti, poslovnih profilov ali izpostavljenosti digitalnemu tveganju. 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 in poslovnim profilom, pristojni organi pa bi morali še naprej ocenjevati in pregledovati pristop takega razdeljevanja.

---

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

36 Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

(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 stroških in izgubah, ki so nastali zaradi motenj na področju IKT, in rezultatih pregledov po incidentu, 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 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[37] in spodbuja vrsto

[37] 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.

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. 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 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, 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 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.

(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 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.

(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, medtem ko bi moral na odpovedi pogodb vplivati vsaj sklop okoliščin, ki kažejo na izpade pri tretjem ponudniku storitev IKT.

(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, zlasti kadar so sklenjeni s tretjimi ponudniki storitev IKT s sedežem v tretji državi. 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. Evropski nadzorni organ, pooblaščen za izvajanje nadzora za vsakega ključnega tretjega ponudnika storitev IKT (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[38].

(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 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

[38] 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.

poslovanja tretjega ponudnika storitev IKT 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, brez dodatnih stroškov ali po ceni, ki je bila predhodno določena.

(53) Pravice do dostopa, inšpekcijskega pregleda in revizije s strani finančnega subjekta ali imenovane tretje osebe so ključni instrumenti pri stalnem spremljanju uspešnosti tretjega ponudnika storitev IKT, ki ga izvaja finančni subjekt, skupaj s polnim sodelovanjem slednjega med inšpekcijskimi pregledi. Tudi pristojni organ finančnega subjekta bi moral imeti na podlagi obvestila pravico do inšpekcijskega pregleda in revizije tretjega ponudnika storitev IKT, ob upoštevanju zaupnosti.

(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 rešitve na kraju samem v skladu z zapletenostjo zagotavljane storitve.

(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.

(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 nadzor. 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, vzpostavljeni na ravni Eurosistema z namenom podpiranja nalog iz člena 127(2) Pogodbe o delovanju Evropske unije.

(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.

(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, pri čemer bi ga podpiral nov pododbor (nadzorniški forum), ki bi izvajal pripravljalno delo za 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 enega od evropskih nadzornih organov imenovati za glavnega nadzornika za vsakega ključnega tretjega ponudnika storitev IKT.

(62) Glavni nadzorniki bi morali imeti potrebna pooblastila za izvajanje preiskav, inšpekcijske preglede ključnih tretjih ponudnikov storitev IKT na kraju samem in zunaj njega, 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.

Podelitev glavne nadzorne pristojnosti evropskim nadzornim organom 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 morali imeti glavni nadzorniki možnost, da predložijo 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 ustrezno upoštevati skladnost s takimi vsebinskimi priporočili glavnih nadzornikov v okviru njihove funkcije v zvezi z bonitetnim nadzorom finančnih subjektov.

(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 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 izkoristili tehnično strokovno znanje strokovnjakov pristojnih organov za upravljanje operativnih tveganj in tveganj na področju IKT, bi morali črpati iz izkušenj nacionalnih nadzornikov in 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 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 zadevnimi pristojnimi organi, vključno z Evropsko centralno banko (ECB) v zvezi s posebnimi nalogami, ki so nanjo prenesene z Uredbo Sveta (EU) št. 1024/2013[39], in posvetovanje z evropskimi nadzornimi organi, in sicer z izmenjavo informacij ter zagotavljanjem pomoči pri nadzornih dejavnostih.

(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 v skladu s členom 290 Pogodbe o delovanju Evropske unije sprejema 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 določenem 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 je pomembno, da se Komisija pri svojem pripravljalnem delu ustrezno posvetuje, vključno na ravni strokovnjakov, in da se ta posvetovanja izvedejo v skladu z načeli iz Medinstitucionalnega sporazuma o boljši pripravi zakonodaje z dne 13. aprila 2016[40]. Za zagotovitev enakopravnega sodelovanja pri pripravi delegiranih

[39] 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).

[40] UL L 123, 12.5.2016, str. 1.

aktov Evropski parlament in Svet zlasti 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[41], vključuje konsolidacijo določb o upravljanju tveganj na področju IKT, ki zajemajo 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 navedene uredbe spremeniti, da se pojasni, da so ustrezne določbe, povezane s tveganji na področju IKT, opredeljene v tej uredbi.

Tehnični standardi bi morali zagotoviti dosledno harmonizacijo zahtev iz te uredbe. Ker imajo evropski nadzorni organi visoko specializirano strokovno znanje, bi morali biti pooblaščeni za pripravo osnutkov regulativnih tehničnih standardov, ki ne vključujejo odločitev politike, in osnutke predložiti Komisiji. Razviti je treba regulativne tehnične standarde na področjih upravljanja tveganj na področju IKT, poročanja, testiranja in ključnih zahtev za dobro spremljanje tveganj tretjih oseb na področju IKT.

(70) Zlasti je pomembno, 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 na način, ki bi ustrezal naravi, obsegu in zapletenosti teh subjektov in njihovih dejavnosti.

(71) Za lažjo primerljivost poročil o večjih incidentih, povezanih z IKT, in zagotovitev preglednosti 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, ki bi določali standardizirane predloge, obrazce in postopke, v skladu 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 velikost in zapletenost 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 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.

---

[41] [*Vstaviti celotni sklic*.]

(73) Ker države članice zaradi potrebe po harmonizaciji 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, in sicer doseganja 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;

   – testiranja digitalne operativne odpornosti;

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

   – ukrepov za dobro upravljanje tveganj tretjih oseb na področju IKT, ki ga izvajajo finančni subjekti;

   (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.

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 kriptoimetij, izdajatelje žetonov, vezanih na sredstva, in izdajatelje pomembnih žetonov, vezanih na sredstva,

(f) centralne depotne družbe,

(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,

(o) institucije za poklicno pokojninsko zavarovanje,

(p) bonitetne agencije,

(q) zakonite revizorje in revizijska podjetja,

(r) upravljavce ključnih referenčnih vrednosti,

(s) ponudnike storitev množičnega financiranja,

(t) repozitorije listinjenja,

(u) tretje ponudnike storitev IKT.

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

Člen 3

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(1) „digitalna operativna odpornost“ pomeni sposobnost finančnega subjekta, da vzpostavi, zagotavlja in pregleduje svojo operativno integriteto s tehnološkega vidika, tako da neposredno ali posredno z uporabo storitev tretjih ponudnikov storitev IKT zagotovi celoten sklop zmogljivosti, povezanih z IKT, ki so potrebne za obravnavo varnosti omrežja in informacijskih sistemov, ki jih uporablja finančni subjekt in ki omogočajo nadaljnje zagotavljanje in kakovost finančnih storitev;

(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 katero koli razumno določljivo okoliščino v zvezi z uporabo omrežja in informacijskih sistemov, vključno z nepravilnim delovanjem, prekoračitvijo zmogljivosti, okvaro, motnjo, oslabitvijo, zlorabo, izgubo ali drugo vrsto zlonamernega ali nenamernega dogodka, ki lahko, če se uresniči, ogrozi varnost omrežja in informacijskih sistemov, orodja ali postopka, odvisnega od tehnologije, delovanja in izvajanja postopka ali zagotavljanja storitev, s čimer ogrozi celovitost ali razpoložljivost podatkov, programske opreme ali katere koli druge komponente storitev in infrastruktur IKT ali povzroči kršitev zaupnosti, škodo na fizični infrastrukturi IKT ali druge škodljive učinke;

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

(6) „incident, povezan z IKT“ pomeni nepredviden ugotovljen dogodek v omrežju in informacijskih sistemih, ki je posledica zlonamerne dejavnosti ali ne ter ki ogroža varnost omrežja in informacijskih sistemov ter informacij, ki jih taki sistemi obdelujejo, shranjujejo ali prenašajo, ali ki ima škodljiv učinek na razpoložljivost, zaupnost, neprekinjenost ali verodostojnost finančnih storitev, ki jih zagotavlja finančni subjekt;

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

(8) „kibernetska grožnja“ pomeni kibernetsko grožnjo, kot je opredeljena v točki 8 člena 2 Uredbe (EU) št. 2019/881 Evropskega parlamenta in Sveta[42];

(9) „kibernetski napad“ pomeni zlonamerni 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;

(11) „obramba v globino“ pomeni strategijo, povezano z IKT, ki vključuje 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 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;

---

[42] 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).

(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 digitalne in podatkovne storitve, vključno s ponudniki storitev računalništva v oblaku, programske opreme, storitev analize podatkov in podatkovnimi centri, 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[43];

(16) „storitve IKT“ pomenijo digitalne in podatkovne storitve, ki se prek sistemov IKT zagotavljajo enemu ali več notranjim ali zunanjim uporabnikom, vključno z zagotavljanjem podatkov, vnosom podatkov, shranjevanjem podatkov, obdelavo podatkov in storitvami poročanja, spremljanjem podatkov ter storitvami za podporo poslovanju in odločanju na podlagi podatkov;

(17) „kritična ali pomembna funkcija“ pomeni funkcijo, katere prekinjeno, pomanjkljivo ali neuspešno izvajanje bi bistveno oviralo stalno skladnost finančnega subjekta s pogoji in obveznostmi njegovega dovoljenja ali drugimi obveznostmi v skladu z veljavno zakonodajo o finančnih storitvah ali pa bi ogrozilo njegovo finančno uspešnost ali trdnost ali neprekinjenost njegovih storitev in dejavnosti;

(18) „ključni tretji ponudnik storitev IKT“ pomeni tretjega ponudnika storitev IKT, imenovanega v skladu s členom 29, za katerega velja okvir nadzora iz členov 30 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, ki nima podjetja/prisotnosti v Uniji 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, ki nima podjetja/prisotnosti v Uniji in ki je sklenil pogodbeni dogovor bodisi s tretjim ponudnikom storitev IKT ali tretjim ponudnikom storitev IKT s sedežem v 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 takih ponudnikov, tako da lahko njihova nedosegljivost, nezmožnost opravljanja storitev ali druga vrsta izpada potencialno ogrozi sposobnost finančnega subjekta in nazadnje celotnega finančnega sistema Unije, da opravlja kritične 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[44], točki (u)

[43] 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).

[44] 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

člena 3(1) Uredbe (EU) 20xx/xx Evropskega parlamenta in Sveta[45] [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[46];

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

(25) „plačilna institucija“ pomeni plačilno institucijo, kot je opredeljena v točki (d) člena 1(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[47];

(27) „centralna nasprotna stranka“ pomeni centralno nasprotno stranko, kot je opredeljena v 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 Direktive (EU) 2016/97;

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

---

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).

45 [*Vstaviti je treba polni naslov in podatke o UL.*]

46 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).

47 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).

(38) „pozavarovalni posrednik“ pomeni pozavarovalnega posrednika, kot je opredeljen v točki 5 člena 2 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 (n) člena 3(1) Uredbe (EU) 202x/xx [*UP: vstaviti je treba sklic na uredbo MiCA*];

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

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

(47) „upravljavec ključnih referenčnih vrednosti“ pomeni upravljavca ključnih referenčnih vrednosti, kot je opredeljen v točki (x) člena x Uredbe xx/202x [*UL: vstavite sklic na uredbo o referenčnih vrednostih*];

(48) „ponudnik storitev množičnega financiranja“ pomeni ponudnika storitev množičnega financiranja, kot je opredeljen v točki (x) člena x Uredbe (EU) 202x/xx [*UP: vstavite 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 podjetje“ pomeni mikro podjetje, kot je opredeljeno v členu 2(3) Priloge k Priporočilu 2003/361/ES.

POGLAVJE II

UPRAVLJANJE TVEGANJ NA PODROČJU IKT

ODDELEK I

Člen 4

Upravljanje in organizacija

1. Finančni subjekti vzpostavijo okvire notranjega upravljanja in nadzora, ki zagotavljajo učinkovito in skrbno upravljanje vseh tveganj na področju IKT.

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;

(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 neprekinjenega poslovanja na področju IKT in načrta okrevanja IKT po katastrofi finančnega subjekta 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 ustrezen proračun, da lahko finančni subjekt izpolnjuje potrebe po digitalni operativni odpornosti v zvezi z vsemi vrstami virov, vključno z usposabljanjem o tveganjih in veščinah na področju IKT za vse ustrezne 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 takih sprememb na kritične ali pomembne funkcije, za katere veljajo navedeni dogovori, vključno s prejetjem povzetka analize tveganja za oceno učinka teh sprememb;

(i) je ustrezno obveščen o 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, sklenjenih s tretjimi ponudniki storitev IKT o uporabi storitev IKT, ali določijo člana višjega vodstva, ki bo odgovoren za nadzor s tem povezane izpostavljenosti tveganju in ustrezne dokumentacije.

4. Člani upravljalnega organa se redno udeležujejo posebnega usposabljanja za pridobitev in obnavljanje zadostnega znanja in spretnosti, da lahko razumejo in ocenijo tveganja na področju IKT ter njihov učinek na poslovanje finančnega subjekta.

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, skladne z njihovimi poslovnimi potrebami, velikostjo in zapletenostjo.

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 zmanjšujejo 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, 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, ter ga redno pregledujejo.

5. Finančni subjekti, ki niso mikro podjetja, zagotovijo ustrezno ločitev 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. Nenehno se izboljšuje na podlagi izkušenj, pridobljenih pri izvajanju in spremljanju.

7. Okvir za upravljanje tveganj na področju IKT iz odstavka 1 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 ter narave, obsega in zapletenosti storitev in dejavnosti finančnih subjektov.

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

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

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

   (c) določa jasne cilje glede informacijske varnosti;

   (d) pojasnjuje referenčne arhitekture IKT in vse spremembe, potrebne za dosego določenih poslovnih ciljev;

(e) opisuje 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) opredeljuje celostno večdobaviteljsko strategijo za IKT na ravni subjektov, ki prikazuje ključne odvisnosti od tretjih ponudnikov storitev IKT in pojasnjuje razloge za uporabo različnih tretjih ponudnikov storitev;

(h) izvaja testiranje digitalne operativne odpornosti;

(i) opisuje komunikacijske strategije v primeru incidentov, povezanih z IKT.

10. Po odobritvi pristojnih organov lahko finančni subjekti naloge preverjanja skladnosti z zahtevami glede upravljanja tveganj na področju IKT prenesejo znotraj skupine ali na zunanja podjetja.

Člen 6

Sistemi, protokoli in orodja IKT

1. Finančni subjekti uporabljajo in vzdržujejo posodobljene sisteme, protokole in orodja IKT, ki izpolnjujejo naslednje pogoje:

(a) sistemi in orodja so skladna z naravo, raznolikostjo, zapletenostjo in obsežnostjo operacij, ki podpirajo izvajanje njihovih dejavnosti;

(b) so zanesljivi;

(c) imajo zadostno zmogljivost, da pravočasno 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 ustrezno spopadajo s potrebami po obdelavi dodatnih informacij, kot se zahteva v stresnih tržnih razmerah ali drugih neugodnih razmerah.

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 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 ustreznost razvrstitve informacijskih sredstev in kakršne koli 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 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, 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 sredstev IKT ter povezave in soodvisnosti med različnimi sredstvi IKT.

5. Finančni subjekti opredelijo in dokumentirajo vse postopke, ki so odvisni od tretjih ponudnikov storitev IKT, in opredelijo medsebojne povezave s tretjimi ponudniki storitev IKT.

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, zlasti pred povezovanjem starih in novih 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 takih tveganj.

2. Finančni subjekti oblikujejo, pridobijo in izvajajo varnostne strategije, politike, postopke, protokole in orodja na področju IKT, katerih cilj je zlasti zagotoviti odpornost, kontinuiteto in razpoložljivost sistemov IKT 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 najsodobnejšo informacijsko in komunikacijsko tehnologijo in postopke, ki:

   (a) zagotavljajo 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 slabim upravljanjem ali tveganji, povezanimi z obdelavo, vključno z neustreznim vodenjem evidenc.

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

(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 virov, podatkov in informacijskih sredstev na področju IKT pri njihovih strankah;

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

(c) izvajajo politike, 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, ter v ta namen vzpostavijo sklop politik, postopkov in kontrol, ki obravnavajo pravice dostopa in njihovo dobro upravljanje;

(d) izvajajo politike in protokole za močne mehanizme avtentikacije, ki temeljijo na ustreznih standardih in namenskih nadzornih sistemih, da se prepreči dostop do kriptografskih ključev, pri čemer se podatki šifrirajo na podlagi rezultatov odobrenih postopkov za razvrščanje podatkov in oceno tveganj;

(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, 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 na način, ki omogoča takojšnjo 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, pri čemer ima ta postopek omogočene 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, ter za opredelitev 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 omogočajo več ravni nadzora, določajo mejne vrednosti opozarjanja in merila za sprožitev postopkov odkrivanja incidentov, povezanih z IKT, in odzivanja nanje ter vzpostavijo samodejne mehanizme opozarjanja za ustrezne zaposlene, odgovorne za odzivanje na incidente, povezane z IKT.

3. Finančni subjekti ob upoštevanju svoje velikosti, poslovanja in profilov tveganja namenijo zadostna sredstva in zmogljivosti za spremljanje dejavnosti uporabnikov, pojavov nepravilnega delovanja na področju IKT in incidentov, povezanih z IKT, zlasti kibernetskih napadov.

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 namensko in celovito politiko neprekinjenega poslovanja na področju IKT, ki je sestavni del operativne politike neprekinjenega poslovanja finančnega subjekta.

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:

   (a) evidentiranje vseh incidentov, povezanih z IKT;

   (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 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 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, ki v primeru aktiviranja njihove politike neprekinjenega poslovanja na področju IKT ali načrta okrevanja IKT po katastrofi določa jasne postopke za upravljanje notranjih in zunanjih obvestil o kriznih razmerah v skladu s členom 13.

7. Finančni subjekti vodijo evidence o dejavnostih pred motnjami in med njimi, ko se aktivira njihova politika neprekinjenega poslovanja na področju IKT ali načrt okrevanja IKT po katastrofi. Take 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 stroških in izgubah, ki nastanejo zaradi motenj na področju IKT in incidentov, povezanih z IKT.

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. 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, katerih operacijsko okolje je drugačno od glavnega, ni neposredno povezano z njim in je varno zaščiteno 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 vzdržujejo redundantne zmogljivosti IKT, opremljene z zmogljivosti virov in funkcionalnostmi, ki so zadostne in ustrezne za zagotavljanje poslovnih potreb.

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 ključnih storitev kot na primarni lokaciji ali zagotoviti raven storitev, potrebnih za zagotovitev, da finančni subjekt opravlja svoje ključne operacije v okviru ciljev obnovitve;

   (c) je takoj dostopna zaposlenim pri finančnem subjektu, da se zagotovi neprekinjenost ključnih storitev, če primarna lokacija za obdelavo postane nedostopna.

6. Finančni subjekti pri določanju ciljev glede časa in točk obnovitve za vsako funkcijo upoštevajo 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, opravijo več pregledov, vključno s postopki usklajevanja, da se zagotovi najvišja raven celovitosti podatkov. 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, ki ustrezajo njihovi velikosti, poslovanju in profilu tveganja, 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 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 finančni subjekti, ki niso mikro podjetja, te spremembe sporočijo pristojnim organom.

   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, 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. Ti veljajo za vse zaposlene in za višje vodstvene delavce.

Finančni subjekti 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 odgovorno razkritje incidentov ali večjih ranljivosti, povezanih z IKT, strankam in partnerjem ter javnosti, kjer je to ustrezno.

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 za 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;

(b) določitev, kako varnostne politike, postopki in orodja IKT iz člena 8(2) vključujejo varnostne kontrole v sisteme od samega začetka (vgrajena varnost), omogočajo prilagoditve glede na spreminjajoče se področje groženj in zagotavljajo uporabo tehnologije obrambe v globino;

(c) nadaljnja opredelitev ustreznih tehnik, metod in protokolov iz točke (b) člena 8(4);

(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).

EBA, ESMA in EIOPA 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.

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 za zagotovitev doslednega in celovitega spremljanja, obravnavanja in nadaljnjega spremljanja incidentov, povezanih z IKT, da se zagotovi prepoznavanje in izkoreninjenje temeljnih vzrokov in s tem se prepreči pojavljanje takih 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 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 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, in podatek, ali je incident, povezan z IKT, vplival na njihov ugled;

   (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 po posvetovanju 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 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.

Evropski nadzorni organi te skupne osnutke regulativnih tehničnih standardov predložijo Komisiji do [*UP: vstaviti datum eno leto 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.

2. Kadar večji incident, povezan z IKT, vpliva ali bi lahko vplival na finančne interese uporabnikov storitev in strank, finančni subjekti uporabnike svojih storitev in stranke nemudoma obvestijo o večjem incidentu, povezanem z IKT, in jih čim prej obvestijo o vseh ukrepih, ki so bili sprejeti za zmanjšanje škodljivih učinkov takega incidenta.

3. Finančni subjekti pristojnemu organu iz člena 41 predložijo:

(a) začetno obvestilo, brez odlašanja, vendar najpozneje do konca delovnega dne, ali, v primeru večjega incidenta, povezanega z IKT, ki se je zgodil pozneje kot dve uri pred koncem delovnega dne, najpozneje štiri ure po začetku naslednjega delovnega dne ali, kadar kanali poročanja niso na voljo, takoj ko postanejo razpoložljivi;

(b) vmesno poročilo najpozneje en teden po začetnem obvestilu iz točke (a), ki mu vsakič, ko je na voljo ustrezna posodobitev statusa, in na posebno zahtevo pristojnega organa sledijo 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 pošiljanja začetnega poročila.

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.

5. Pristojni organ po prejemu poročila iz odstavka 1 brez nepotrebnega odlašanja sporoči podrobnosti o incidentu 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.

6. EBA, ESMA ali EIOPA in ECB 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;

(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) odstavka 1 in skupne osnutke izvedbenih tehničnih standardov iz točke (b)

odstavka 1 predložijo Komisiji do xx 202x [*UP: vstaviti datum eno leto po datumu začetka veljavnosti*].

Na Komisijo se prenese pooblastilo za dopolnitev te uredbe s sprejetjem skupnih regulativnih tehničnih standardov iz točke (a) odstavka 1 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) odstavka 1 v skladu s členom 15 Uredbe (EU) št. 1093/2010, (EU) št. 1095/2010 oziroma (EU) št. 1094/2010.

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 takega vozlišča EU;

   (b) koristi, omejitve in možna tveganja;

   (c) elemente operativnega upravljanja;

   (d) pogoje članstva;

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

   (f) predhodno oceno finančnih stroškov, povezanih z vzpostavitvijo operativne platforme za podporo 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.

2. Evropski nadzorni organi prek Skupnega odbora enkrat letno na anonimizirani in združeni podlagi poročajo o obvestilih o 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, 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.

POGLAVJE IV

TESTIRANJE DIGITALNE OPERATIVNE ODPORNOSTI

Člen 21

Splošne zahteve za izvajanje testiranja digitalne operativne odpornosti

1. Finančni subjekti za namene ocenjevanja pripravljenosti na incidente, povezane z IKT, opredelitve 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, pri čemer upoštevajo svojo velikost, poslovanje in profil tveganja.

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.

5. Finančni subjekti vzpostavijo postopke in politike za prednostno obravnavo, razvrstitev in odpravo 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 vsaj enkrat letno testirajo vse ključne sisteme 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, vključno z ocenami in pregledi ranljivosti, analizami odprtokodne programske opreme, ocenami varnosti omrežja, analizami vrzeli, pregledi fizične varnosti, vprašalniki in rešitvami za preiskovanje programske opreme, pregledi izvorne kode, kjer je to mogoče, testiranji na podlagi scenarijev, testi združljivosti, testi učinkovitosti, celovitim testiranjem ali penetracijskim testiranjem.

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 odstavkom 4, vsaj vsaka tri leta izvedejo napredno penetracijsko testiranje na podlagi analize groženj.

2. Penetracijsko testiranje na podlagi analize groženj zajema vsaj kritične funkcije in storitve finančnega subjekta ter se izvaja na aktivnih produkcijskih sistemih, ki podpirajo take funkcije. Natančen obseg penetracijskega testiranja na podlagi analize groženj, ki temelji na oceni kritičnih funkcij in storitev, določijo finančni subjekti in potrdijo pristojni organi.

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

   Kadar so tretji ponudniki storitev IKT vključeni v penetracijsko testiranje na podlagi analize groženj, finančni subjekt sprejme potrebne ukrepe, da zagotovi sodelovanje teh ponudnikov.

   Finančni subjekti uporabljajo učinkovite kontrole za upravljanje tveganj, da zmanjšajo tveganja morebitnega učinka na podatke, škode na sredstvih in motenj v ključnih storitvah 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 pristojnemu organu predložijo dokumentacijo, ki potrjuje, da je bilo penetracijsko testiranje na podlagi analize groženj izvedeno v skladu z zahtevami. Pristojni organi potrdijo dokumentacijo in izdajo potrdilo.

3. Finančni subjekti sklenejo pogodbo s preizkuševalci v skladu s členom 24 za namene izvajanja penetracijskega testiranja na podlagi analize groženj.

   Pristojni organi finančne subjekte, ki izvedejo penetracijsko testiranje na podlagi analize groženj, opredelijo na način, ki je skladen z velikostjo, obsegom, dejavnostjo in splošnim profilom tveganja finančnega subjekta, 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.

4. EBA, ESMA in EIOPA po posvetovanju z ECB in ob upoštevanju ustreznih okvirov v Uniji, ki veljajo za penetracijsko testiranje na podlagi obveščevalnih podatkov, pripravijo osnutke regulativnih tehničnih standardov, v katerih podrobneje opredelijo:

   (a) merila, ki veljajo za namene uporabe odstavka 6 tega člena;

   (b) zahteve v zvezi z:

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

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

(c) rezultati ter zaključno fazo in fazo sanacije;

(c) vrsto sodelovanja nadzornih organov, ki je potrebno za izvedbo penetracijskega testiranja na podlagi analize groženj pri finančnih subjektih, ki delujejo v več kot eni državi članici, 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 dva meseca 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 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;

(d) če gre za zunanje preizkuševalce, 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) če gre za zunanje preizkuševalce, imajo polno kritje z ustreznimi zavarovanji poklicne odgovornosti, vključno s kritjem za tveganje kršitve in malomarnosti.

2. Finančni subjekti zagotovijo, da se v sporazumih, 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) 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.

3. Finančni subjekti v sklopu svojega okvira za upravljanje tveganj na področju IKT sprejmejo in redno pregledujejo strategijo o tveganju tretjih oseb na področju IKT, pri čemer upoštevajo večdobaviteljsko strategijo iz točke (g) člena 5(9). 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 jih zagotavljajo tretji ponudniki storitev IKT.

   Pogodbeni dogovori iz prvega pododstavka se ustrezno dokumentirajo, pri čemer se razlikuje med tistimi, ki zajemajo kritične ali pomembne funkcije, in tistimi, ki ne zajemajo takih funkcij.

Finančni subjekti pristojnim organom vsaj enkrat letno poročajo o številu novih dogovorov o uporabi storitev IKT, 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 najnovejše standarde informacijske varnosti.

7. Finančni subjekti pri uveljavljanju pravic do dostopa, inšpekcijskih pregledov in revizij pri tretjem ponudniku storitev IKT 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 visoko stopnjo tehnološke zapletenosti, 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 se pogodbeni dogovori o uporabi storitev IKT prekinejo vsaj v naslednjih okoliščinah:

   (a) kršitev veljavnih zakonov, predpisov ali pogodbenih pogojev s strani tretjega ponudnika 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 pri njegovem splošnem upravljanju tveganj na področju IKT 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 ne more več učinkovito nadzirati finančnega subjekta.

9. Finančni subjekti vzpostavijo izhodne strategije, da 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.

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 eno leto po datumu 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 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 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 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 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, zlasti v primeru podizvajalca storitev IKT s sedežem v tretji državi.

   Kadar se pogodbeni dogovori o uporabi storitev IKT sklenejo s tretjim ponudnikom storitev IKT s sedežem v tretji državi, finančni subjekti za pomembne štejejo vsaj naslednje dejavnike:

   (a) spoštovanje varstva podatkov;

   (b) učinkovito izvrševanje zakonodaje;

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

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

   Finančni subjekti ocenijo, ali in kako lahko potencialno dolge ali zapletene verige podizvajanja vplivajo na njihovo zmožnost popolnega spremljanja pogodbenih funkcij in na 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 enem pisnem dokumentu, ki je na voljo strankam v papirni obliki ali obliki, ki jo je mogoče prenesti in do nje dostopati.

2. 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, kjer se bodo zagotavljale pogodbene funkcije in storitve, oddane v izvajanje ali podizvajanje, in obdelovali podatki, vključno z lokacijo hrambe, ter zahtevo, da tretji ponudnik storitev IKT obvesti finančnega subjekta, če namerava spremeniti te lokacije;

(c) določbe o dostopnosti, razpoložljivosti, celovitosti, varnosti in zaščiti osebnih podatkov ter 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;

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

(f) obveznost tretjega ponudnika storitev IKT, da v primeru incidenta, 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 ustrezno zagotavljajo varno opravljanje storitev v skladu z njegovim regulativnim okvirom;

(h) 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 kopiranja ustrezne dokumentacije, 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) zavezanost popolnemu sodelovanju med inšpekcijskimi pregledi na kraju samem, ki jih izvaja finančni subjekt, ter podrobnosti o obsegu, načinih in pogostosti revizij na daljavo;

(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;

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

(a) med katerim bo tretji ponudnik storitev IKT še naprej zagotavljal ustrezne funkcije ali storitve, da bi zmanjšal tveganje motenj pri finančnem subjektu;

(b) 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.

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

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 te osnutke regulativnih tehničnih standardov Komisiji predložijo do [*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 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 foruma, ustanovljenega v skladu s členom 29(1):

(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.

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.

3. Komisiji se v skladu s členom 50 podeli pooblastilo za sprejetje delegiranih aktov za dopolnitev 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. Evropski nadzorni organi prek Skupnega odbora pripravijo, objavijo in vsako leto posodobijo 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) nadzorniškemu forumu, ustanovljenemu v skladu s členom 29. Nadzorniški forum 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.

9. Finančni subjekti ne smejo uporabljati tretjega ponudnika storitev IKT s sedežem v tretji državi, ki bi bil v skladu s točko (a) odstavka 1 določen za ključnega, če bi bil ustanovljen v Uniji.

Člen 29

Struktura nadzornega okvira

1. Skupni odbor v skladu s členom 57 uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010 ustanovi nadzorniški forum kot pododbor, ki podpira naloge Skupnega odbora in glavnega nadzornika iz točke (b) člena 28(1) na področju tveganj tretjih oseb na področju IKT v finančnih sektorjih. Nadzorniški forum pripravi osnutke skupnih stališč in skupnih aktov Skupnega odbora na navedenem področju.

Nadzorniški forum 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. Nadzorniški forum 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.

3. Nadzorniški forum 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.

4. Nadzorniški forum je sestavljen iz predsednikov evropskih nadzornih organov in enega predstavnika na visoki ravni, ki je izbran med osebjem, zaposlenim v ustreznem pristojnem organu iz vsake države članice. Izvršni direktorji vsakega evropskega nadzornega organa in po en predstavnik Evropske komisije ter ESRB, ECB in ENISA sodelujejo v nadzorniškem forumu kot opazovalci.

5. Evropski nadzorni organi v skladu s členom 16 uredb (EU) št. 1093/2010, (EU) št. 1094/2010 in (EU) št. 1095/2010 izdajo smernice o sodelovanju med evropskimi nadzornimi organi in pristojnimi organi za namene tega oddelka v zvezi s podrobnimi postopki in pogoji glede izvajanja nalog med pristojnimi organi in evropskimi nadzornimi organi ter glede podrobnosti o izmenjavi informacij, ki jih pristojni organi potrebujejo za zagotovitev nadaljnjega ukrepanja na podlagi priporočil, ki jih glavni nadzorniki naslovijo na ključne tretje ponudnike storitev IKT v skladu s točko (d) člena 31(1).

6. 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.

7. Evropski nadzorni organi prek Skupnega odbora in na podlagi pripravljalnega dela, ki ga izvede nadzorniški forum, enkrat letno Evropskemu parlamentu, Svetu in Komisiji predložijo poročilo o uporabi tega oddelka.

Člen 30

Naloge glavnega nadzornika

1. 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.

2. Ocena iz odstavka 1 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 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. Glavni nadzornik na podlagi ocene iz odstavka 1 sprejme jasen, podroben in obrazložen individualni načrt nadzora za vsakega ključnega tretjega ponudnika storitev IKT. Ta načrt se vsako leto posreduje ključnemu tretjemu ponudniku storitev IKT.

4. Ko so letni načrti nadzora iz odstavka 3 potrjeni in posredovani ključnih tretjim ponudnikom storitev IKT, lahko pristojni organi sprejmejo ukrepe v zvezi s ključnimi tretjimi ponudniki storitev IKT samo v dogovoru z glavnim nadzornikom.

Člen 31

Pooblastila glavnega nadzornika

1. Za namene izvajanja nalog, določenih v tem oddelku, ima glavni nadzornik naslednja pooblastila:

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

   (b) da izvaja splošne preiskave in inšpekcijske preglede 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 točke (d) tega odstavka;

   (d) 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 glavni nadzornik 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 glavni nadzornik 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, glavni nadzornik 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;

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

2. Glavni nadzornik se pred izvrševanjem pooblastil iz odstavka 1 posvetuje z nadzorniškim forumom.

3. Ključni tretji ponudniki storitev IKT v dobri veri sodelujejo z glavnim nadzornikom in mu pomagajo pri izpolnjevanju njegovih nalog.

4. Glavni nadzornik lahko naloži periodično denarno kazen, da prisili ključnega tretjega ponudnika storitev IKT, da upošteva točke (a), (b) in (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 1 % povprečnega dnevnega svetovnega prometa ključnega tretjega ponudnika storitev IKT 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.

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. Pri zahtevi po predložitvi 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 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;

(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 34(1) opravi potrebne preiskave tretjih ponudnikov storitev IKT.

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) pridobi 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 s katero koli drugo fizično ali pravno osebo, ki privoli 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.

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 pomembnih sistemov, omrežij, naprav, informacij in podatkov na področju IKT, ki se uporabljajo za zagotavljanje storitev finančnim subjektom ali prispevajo k njihovemu zagotavljanju.

5. Pred kakršnim koli načrtovanim obiskom na kraju samem glavni nadzorniki o njem 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 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 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. Glavni nadzornik v treh mesecih po zaključku preiskave ali inšpekcijskega pregleda na kraju samem in po posvetovanju z nadzorniškim forumom 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 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 glavnih nadzornikov v skladu s členom 37(2).

2. Evropski nadzorni organi te osnutke regulativnih tehničnih standardov predložijo Komisiji 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 izdajo glavni nadzorniki v skladu s točko (d) člena 31(1), ključni tretji ponudniki storitev IKT glavnega nadzornika obvestijo, ali nameravajo upoštevati ta priporočila. Glavni nadzorniki te informacije takoj posredujejo pristojnim organom.

2. Pristojni organi spremljajo, ali finančni subjekti upoštevajo tveganja, opredeljena v priporočilih, ki jih je glavni nadzornik naslovil na ključne tretje ponudnike storitev IKT v skladu s točko (d) člena 31(1).

3. Pristojni organi lahko v skladu s členom 44 od finančnih subjektov zahtevajo, da bodisi delno bodisi v celoti začasno ustavijo uporabo ali uvajanje storitve, ki jo zagotavlja ključni tretji ponudnik storitev IKT, dokler tveganja, opredeljena v priporočilih, naslovljenih na ključne tretje ponudnike storitev IKT, niso obravnavana. Po potrebi lahko od finančnih subjektov zahtevajo, da delno ali v celoti prekinejo ustrezne pogodbene dogovore, sklenjene s ključnimi tretjimi ponudniki storitev IKT.

4. Pri sprejemanju odločitev iz odstavka 3 pristojni organi upoštevajo 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.

5. Pristojni organi glavne nadzornike redno obveščajo o pristopih in ukrepih, sprejetih pri njihovih nadzornih nalogah v zvezi s finančnimi subjekti, ter o pogodbenih ukrepih, ki jih ti sprejmejo, kadar ključni tretji ponudniki storitev IKT niso delno ali v celoti sprejeli priporočil glavnih nadzornikov.

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 upravne stroške in je sorazmeren z njegovim prometom.

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 lahko med seboj izmenjujejo informacije in obveščevalne podatke o kibernetskih grožnjah, 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, zlasti z ozaveščanjem v zvezi s kibernetskimi grožnjami, k omejevanju ali oviranju zmožnosti širjenja kibernetskih groženj ter podpiranju vrste obrambnih zmogljivosti, tehnik odkrivanja groženj, blažilnih ukrepov ali faz odzivanja in okrevanja finančnih subjektov;

   (b) poteka v zaupanja vrednih skupnostih finančnih subjektov;

(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[48] in smernic o politiki konkurence[49].

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.

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 kriptoimetij, izdajatelje 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 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;

---

[48] 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).

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

(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 poklicno pokojninsko zavarovanje 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 xx/202x*;

(r) za ponudnike storitev množičnega financiranja pristojni organ, imenovan v skladu s *členom x Uredbe xx/202x*;

(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, lahko evropski nadzorni organi in pristojni organi zaprosijo, da jih povabijo k delu skupine za sodelovanje.

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.

Člen 43

Finančne medsektorske vaje, obveščanje in sodelovanje

1. Evropski nadzorni organi lahko prek Skupnega odbora in v sodelovanju s pristojnimi organi, ECB 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 s tem povezane 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 in ECB tesno sodelujejo 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 pristojni organ meni, da je v nasprotju z določbami te uredbe, in preprečijo, da bi se taka praksa ali ravnanje ponovilo;

   (c) sprejmejo kakršni koli 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 eno leto 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, identiteti odgovornih oseb ter naloženih kaznih.

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 pooblastila

1. Pooblastilo za sprejemanje delegiranih aktov se prenese 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*].

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 njegovi objavi v *Uradnem listu Evropske unije* ali na poznejši dan, ki je določen v njem. 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 dveh 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 dva meseca.

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 in Evropskemu parlamentu in Svetu predloži poročilo ter mu po potrebi priloži zakonodajni predlog v zvezi z merili za imenovanje ključnih tretjih ponudnikov storitev IKT iz člena 28(2).

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].“;

(4) v odstavku 6 se prvi pododstavek nadomesti z naslednjim:

„CDD odkriva, spremlja in upravlja tveganja, ki jih za njeno poslovanje morda pomenijo ključni udeleženci v sistemih poravnave vrednostnih papirjev, ki jih upravlja, ter izvajalci javnih in drugih storitev in druge CDD ali druge tržne infrastrukture. Pristojnim in zadevnim organom na zahtevo zagotovi informacije o vsakem takem odkritem tveganju. Hkrati pristojni organ in zadevne organe brez odlašanja obvesti o vseh operativnih incidentih, ki so posledica takih tveganj, razen o incidentih, povezanih s tveganjem na področju IKT.“;

(5) v odstavku 7 se prvi pododstavek nadomesti z naslednjim:

„ESMA v tesnem sodelovanju s članicami ESCB pripravi osnutke regulativnih tehničnih standardov, da se določijo operativna tveganja iz odstavkov 1 in 6, razen tveganj na področju IKT, ter metode za testiranje, obravnavo ali zmanjšanje teh tveganj, vključno s politikami neprekinjenega poslovanja in načrti ponovne vzpostavitve delovanja iz odstavkov 3 in 4 ter metodami za njihovo oceno.“

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 12 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.

V Bruslju,

Za Evropski parlament	*Za Svet*
Predsednik	*Predsednik*

OCENA FINANČNIH POSLEDIC ZAKONODAJNEGA PREDLOGA

1. OKVIR PREDLOGA/POBUDE

1.1 Naslov predloga/pobude

1.2 Zadevna področja

1.3 Vrsta predloga/pobude

1.4 Cilji

1.5 Utemeljitev predloga/pobude

1.6 Trajanje predloga/pobude in finančnih posledic

1.7 Načrtovani načini upravljanja

2. UKREPI UPRAVLJANJA

2.1 Pravila o spremljanju in poročanju

2.2 Upravljavski in kontrolni sistemi

2.3 Ukrepi za preprečevanje goljufij in nepravilnosti

3. OCENA FINANČNIH POSLEDIC PREDLOGA/POBUDE

3.1 Zadevni razdelki večletnega finančnega okvira in odhodkovne proračunske vrstice

3.2 Ocenjene posledice za odhodke

3.2.1 Povzetek ocenjenih posledic za odhodke

3.2.2 Ocenjene posledice za odobritve

3.2.3 Ocenjene posledice za človeške vire

3.2.4 Skladnost z veljavnim večletnim finančnim okvirom

3.2.5 Udeležba tretjih oseb pri financiranju

3.3 Ocenjene posledice za prihodke

Priloga

Splošne predpostavke

Nadzorna pooblastila

OCENA FINANČNIH POSLEDIC ZAKONODAJNEGA PREDLOGA – „AGENCIJE“

1. OKVIR PREDLOGA/POBUDE

1.1. Naslov predloga/pobude

Predlog uredbe Evropskega parlamenta in Sveta o digitalni operativni odpornosti finančnega sektorja.

1.2. Zadevna področja

Področje: Finančna stabilnost, finančne storitve in unija kapitalskih trgov

Dejavnost: Digitalna operativna odpornost

1.3. Ukrep, na katerega se predlog nanaša

☑ **Nov ukrep**

☐ **Nov ukrep na podlagi pilotnega projekta / pripravljalnega ukrepa**[50]

☐ **Podaljšanje obstoječega ukrepa**

☐ **Združitev enega ali več ukrepov za oblikovanje drugega/novega ukrepa**

1.4. Cilji

1.4.1. Splošni cilji

Splošni cilj pobude je okrepiti digitalno operativno odpornost subjektov finančnega sektorja EU z racionalizacijo in nadgradnjo obstoječih pravil ter uvajanjem novih zahtev v primeru vrzeli. To bi okrepilo tudi digitalno razsežnost enotnih pravil.

Skupni cilj je mogoče razdeliti na tri splošne cilje: (1) zmanjšati tveganje finančnih motenj in nestabilnosti, (2) zmanjšati upravno breme in povečati učinkovitost nadzora ter (3) povečati zaščito potrošnikov in vlagateljev.

1.4.2. Specifični cilji

Specifični cilji predloga so:

celoviteje obravnavati tveganja na področju informacijske in komunikacijske tehnologije (IKT) in okrepiti splošno stopnjo digitalne odpornosti finančnega sektorja;

racionalizirati poročanje o incidentih, povezanih z IKT, in obravnavati prekrivajoče se zahteve glede poročanja;

omogočiti finančnim nadzornikom dostop do informacij o incidentih, povezanih z IKT;

zagotoviti, da finančni subjekti, ki jih zajema ta predlog, ocenijo učinkovitost svojih preventivnih ukrepov in ukrepov za odpornost ter prepoznajo ranljivosti, povezane z IKT;

zmanjšati razdrobljenost enotnega trga in omogočiti čezmejno sprejemanje rezultatov testiranja;

[50] V skladu s členom 58(2)(a) ali (b) finančne uredbe.

okrepiti pogodbene zaščitne ukrepe za finančne subjekte, ko uporabljajo storitve IKT, vključno s pravili za oddajo v zunanje izvajanje (ki urejajo spremljanje tretjih ponudnikov storitev IKT); zagotoviti nadzor nad dejavnostmi ključnih tretjih ponudnikov storitev IKT; spodbuditi izmenjavo obveščevalnih podatkov o grožnjah v finančnem sektorju.

1.4.3. Pričakovani rezultati in posledice

Navedite, kakšne posledice naj bi imel(-a) predlog/pobuda za upravičence/ciljne skupine.

Zakon o digitalni operativni odpornosti za finančni sektor bi zagotovil celovit okvir, ki bi zajemal vse vidike digitalne operativne odpornosti, in bi uspešno izboljšal splošno operativno odpornost finančnega sektorja. Zagotavljal bi jasnost in skladnost v okviru enotnih pravil.

Prav tako bi omogočil jasnejšo in skladnejšo povezanost z direktivo o kibernetski varnosti in njenim pregledom. Finančnim subjektom bi prinesel jasnost glede različnih pravil o digitalni operativni odpornosti, ki jih morajo upoštevati, zlasti tistim finančnim subjektom, ki imajo več dovoljenj in poslujejo na različnih trgih v EU.

1.4.4. Kazalniki smotrnosti

Navedite, s katerimi kazalniki se bodo spremljali napredek in dosežki.

Mogoči kazalniki:

število incidentov, povezanih z IKT, v finančnem sektorju EU in njihov učinek;

število večjih incidentov, povezanih z IKT, o katerih se je poročalo bonitetnim nadzornikom;

število finančnih subjektov, ki bi morali izvajati penetracijsko testiranje na podlagi analize groženj;

število finančnih subjektov, ki uporabljajo standardne pogodbene klavzule za sklepanje pogodbenih dogovorov s tretjimi ponudniki storitev IKT;

število ključnih tretjih ponudnikov storitev IKT, ki jih nadzorujejo evropski nadzorni organi / bonitetni nadzorniki;

število finančnih subjektov, ki sodelujejo v rešitvah za izmenjavo obveščevalnih podatkov o grožnjah;

število organov, ki prejmejo poročila o istem incidentu, povezanem z IKT;

število čezmejnih penetracijskih testiranj na podlagi analize groženj.

1.5. Utemeljitev predloga/pobude

1.5.1. Potrebe, ki jih je treba zadovoljiti kratkoročno ali dolgoročno, vključno s podrobno časovnico za uvajanje ustreznih ukrepov za izvajanje pobude

Finančni sektor se močno zanaša na informacijske in komunikacijske tehnologije (IKT). Kljub znatnemu napredku, ki je bil dosežen z nacionalnimi in evropskimi ciljno usmerjenimi političnimi in zakonodajnimi pobudami, tveganja na področju IKT še naprej predstavljajo izziv za operativno odpornost, uspešnost in stabilnost finančnega sistema EU. Reforma, ki je sledila finančni krizi leta 2008, je predvsem okrepila finančno odpornost finančnega sektorja EU ter si prizadevala zaščititi konkurenčnost in stabilnost EU z vidika gospodarstva, bonitetnega vidika in vidika ravnanja na trgu. Varnost IKT in splošna digitalna operativna odpornost sta del operativnega tveganja, vendar nista bili v ospredju regulativnega programa po krizi in sta se razvili le na nekaterih področjih politike finančnih trgov in ureditve EU ali le v nekaterih državah članicah. To se kaže v naslednjih izzivih, ki bi jih moral obravnavati predlog:

Pravni okvir EU, ki zajema tveganja na področju IKT in operativno odpornost v finančnem sektorju, je razdrobljen in ni v celoti usklajen.

Ker ni usklajenih zahtev glede poročanja o incidentih, povezanih z IKT, nadzorniki nimajo celovitega pregleda nad naravo, pogostostjo, pomenom in učinkom incidentov.

Nekateri finančni subjekti se soočajo z zapletenimi, prekrivajočimi se in potencialno neskladnimi zahtevami glede poročanja za isti incident, povezan z IKT.

Nezadostna izmenjava informacij in sodelovanje na področju obveščevalnih podatkov o kibernetskih grožnjah na strateški, taktični in operativni ravni posameznim finančnim subjektom preprečuje, da bi ustrezno ocenjevali in spremljali kibernetske grožnje, se branili pred njimi in se odzivali nanje.

V nekaterih finančnih podsektorjih so lahko okviri za penetracijsko testiranje in testiranje odpornosti številni in neusklajeni, pri čemer se rezultati ne priznajo čezmejno, medtem ko drugi podsektorji nimajo takih okvirov za testiranje.

Zaradi pomanjkanja nadzorniškega vpogleda v dejavnosti finančnih subjektov, ki jih zagotavljajo tretji ponudniki storitev IKT, so posamezni finančni subjekti in celotni finančni sistem izpostavljeni operativnim tveganjem.

Finančni nadzorniki nimajo zadostnega pooblastila ali orodij za spremljanje in upravljanje tveganj koncentracije in sistemskih tveganj, ki izhajajo iz odvisnosti finančnih subjektov od tretjih oseb na področju IKT.

1.5.2. Dodana vrednost ukrepanja Unije (ki je lahko posledica različnih dejavnikov, npr. usklajevalnih koristi, pravne varnosti, večje učinkovitosti ali dopolnjevanja). Za namene te točke je „dodana vrednost ukrepanja Unije“ vrednost, ki izhaja iz ukrepanja Unije in predstavlja dodatno vrednost poleg tiste, ki bi jo sicer ustvarile države članice same.

Razlogi za ukrepanje na evropski ravni (predhodno):

Digitalna operativna odpornost je vprašanje skupnega interesa za finančne trge v EU. Ukrepi na ravni EU bi prinesli več prednosti in višjo vrednost kot ločeni ukrepi na nacionalni ravni. Če se ne bi dodale te operativne določbe o tveganjih na področju IKT, bi enotna pravila zagotavljala orodja za upravljanje vseh drugih vrst tveganj na evropski ravni, vendar ne bi zajemala vidikov digitalne operativne odpornosti ali pa bi jih prepustila razdrobljenim in neusklajenim pobudam na nacionalni ravni. Predlog bi zagotovil pravno jasnost o tem, ali in kako se uporabljajo digitalne operativne določbe, zlasti za čezmejne finančne subjekte, in odpravil potrebo, da države članice posamezno izboljšajo pravila, standarde in pričakovanja glede operativne odpornosti in kibernetske varnosti kot odziv na trenutno omejen obseg pravil EU in splošno naravo direktive o kibernetski varnosti.

Pričakovana ustvarjena dodana vrednost Unije (naknadno):

Posredovanje Unije bi znatno povečalo učinkovitost politike ter hkrati zmanjšalo zapletenost ter olajšalo finančno in upravno breme za vse finančne subjekte. Uskladilo bi področje gospodarstva, ki je globoko medsebojno povezano in integrirano ter ima že koristi od enotnega sklopa pravil in nadzora. Kar zadeva poročanje o incidentih, povezanih z IKT, bi predlog zmanjšal breme poročanja in znižal implicitne stroške, ki nastajajo, ker se o istem incidentu, povezanem z IKT, poroča različnim organom EU in/ali nacionalnim organom. Prav tako bo omogočil vzajemno priznavanje/sprejemanje rezultatov testiranja subjektov, ki poslujejo čezmejno in za katere veljajo različni okviri testiranja v različnih državah članicah.

1.5.3. Spoznanja iz podobnih izkušenj v preteklosti

Nova pobuda

1.5.4. Skladnost z večletnim finančnim okvirom in možne sinergije z drugimi ustreznimi instrumenti

Cilj tega predloga je skladen s številnimi drugimi politikami in tekočimi pobudami EU, zlasti z direktivo o varnosti omrežij in informacij (NIS) in direktivo o evropski kritični infrastrukturi. Predlog bi ohranil koristi, povezane s horizontalnim okvirom za kibernetsko varnost, saj bi trije finančni podsektorji še naprej spadali na področje uporabe direktive o kibernetski varnosti. Če bi se ohranila povezanost z ekosistemom direktive o kibernetski varnosti, bi si finančni nadzorniki lahko izmenjevali pomembne informacije z organi NIS in sodelovali v skupini za sodelovanje na področju varnosti omrežij in informacij. Predlog ne bi vplival na direktivo o kibernetski varnosti, temveč bi temeljil na njej in odpravljal morebitna prekrivanja z izjemo *lex specialis*. Povezanost med uredbo o finančnih storitvah in direktivo o kibernetski varnosti bi še naprej urejala klavzula *lex specialis*, s čimer bi bili finančni subjekti izvzeti iz vsebinskih zahtev v direktivi o kibernetski varnosti in bi se preprečilo prekrivanje med obema aktoma. Poleg tega je predlog skladen z direktivo o evropski kritični infrastrukturi, ki se trenutno pregleduje, da bi se izboljšali zaščita in odpornost kritične infrastrukture pred nekibernetskimi grožnjami.

Predlog ne bi vplival na večletni finančni načrt. Prvič, okvir nadzora nad ključnimi tretjimi ponudniki storitev IKT bo v celoti financiran z nadomestili, ki se zaračunavajo tem ponudnikom; drugič, dodatne regulativne naloge v zvezi z digitalno operativno odpornostjo, zaupane evropskim nadzornim organom, bodo zagotovljene z notranjo prerazporeditvijo obstoječega osebja.

To pomeni predlog za povečanje pooblaščenega osebja agencije v prihodnjem letnem proračunskem postopku. Agencija si bo še naprej prizadevala za čim večjo sinergijo in povečanje učinkovitosti (med drugim prek informacijskih sistemov) in natančno spremljala dodatno delovno obremenitev, povezano s tem predlogom, ki bi se kazala v številu pooblaščenih zaposlenih, ki jih agencija zahteva v letnem proračunskem postopku.

1.5.5. Ocena različnih razpoložljivih možnosti financiranja, vključno z možnostmi za prerazporeditev

Obravnavanih je bilo več možnosti financiranja:

Prvič, dodatni stroški bi se lahko financirali z običajnim mehanizmom financiranja evropskih nadzornih organov. Vendar bi to pomenilo znatno povečanje prispevka EU k finančnim virom evropskih nadzornih organov.

Ta možnost se izbere za stroške, ki izhajajo iz regulativnih nalog, povezanih s tem predlogom. Evropski nadzorni organi bodo pozvani k prerazporeditvi obstoječega osebja, da bi se razvili številni tehnični standardi. Vendar dodatnih stroškov, povezanih z nadzorom ključnih tretjih ponudnikov storitev, ni bilo mogoče pokriti s prerazporeditvijo virov znotraj evropskih nadzornih organov, ki imajo poleg nalog, predvidenih v tem predlogu in drugih zakonodajnih aktih Unije, še druge naloge. Poleg tega nadzorniške naloge, povezane z digitalno operativno odpornostjo, zahtevajo posebno tehnično in strokovno znanje. Ker trenutna raven takih virov v evropskih nadzornih organih ni zadostna, so potrebni dodatni viri.

Nazadnje, v skladu s predlogom se bodo zaračunavala nadomestila ključnim tretjim ponudnikom storitev IKT, ki so predmet nadzora. Ta nadomestila so namenjena kritju vseh dodatnih virov, ki jih evropski nadzorni organi potrebujejo za izvajanje svojih novih nalog in pooblastil.

1.6. Trajanje predloga/pobude in finančnih posledic

☐ **Časovno omejeno**

☐ trajanje predloga/pobude od [DD. MM.] LLLL do [DD. MM.] LLLL,

☐ finančne posledice med letoma LLLL in LLLL.

☑ **Časovno neomejeno**

izvajanje z obdobjem uvajanja od leta 2021,

ki mu sledi izvajanje v celoti.

1.7. Načrtovani načini upravljanja[51]

Neposredno upravljanje – Komisija:

☐ prek izvajalskih agencij.

☐ **Deljeno upravljanje** z državami članicami.

☑ **Posredno upravljanje** tako da se naloge izvrševanja proračuna poverijo:

☐ mednarodnim organizacijam in njihovim agencijam (navedite),

☐ EIB in Evropskemu investicijskemu skladu,

☑ organom iz členov 70 in 71,

☐ subjektom javnega prava,

☐ subjektom zasebnega prava, ki opravljajo javne storitve, kolikor ti subjekti zagotavljajo ustrezna finančna jamstva,

☐ subjektom zasebnega prava države članice, ki so pooblaščeni za izvajanje javno-zasebnih partnerstev in ki zagotavljajo ustrezna finančna jamstva,

☐ osebam, pooblaščenim za izvajanje določenih ukrepov SZVP na podlagi naslova V PEU in opredeljenim v zadevnem temeljnem aktu.

Opombe

Ni relevantno.

[51] Pojasnila o načinih upravljanja in sklici na finančno uredbo so na voljo na spletišču BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. UKREPI UPRAVLJANJA

2.1. Pravila o spremljanju in poročanju

Navedite pogostost in pogoje.

V skladu z že obstoječimi ureditvami evropski nadzorni organi pripravljajo redna poročila o svoji dejavnosti (vključno z notranjim poročanjem višjemu vodstvu, poročanjem odborom in pripravo letnega poročila) in so predmet revizij uporabe sredstev in smotrnosti poslovanja, ki jih opravljata Računsko sodišče in Služba Komisije za notranjo revizijo. Spremljanje ukrepov, vključenih v predlog, in poročanje o njih, bo skladno z že obstoječimi zahtevami, pa tudi z morebitnimi novimi zahtevami, ki bi izhajale iz tega predloga.

2.2. Upravljavski in kontrolni sistemi

2.2.1. Utemeljitev načinov upravljanja, mehanizmov financiranja, načinov plačevanja in predlagane strategije kontrol

Upravljanje bo posredno, prek evropskih nadzornih organov. Mehanizem financiranja bi se izvajal z nadomestili, zaračunanimi ključnim tretjim ponudnikom storitev IKT.

2.2.2. Podatki o ugotovljenih tveganjih in vzpostavljenih sistemih notranjih kontrol za njihovo zmanjševanje

V zvezi z zakonito, gospodarno, učinkovito in uspešno uporabo odobritev, ki izhajajo iz predloga, se pričakuje, da predlog ne bi prinesel bistvenih novih tveganj, ki jih ne zajema obstoječi okvir za notranji nadzor. Vendar je lahko nov izziv povezan z zagotavljanjem pravočasne pridobitve nadomestil od zadevnih ključnih tretjih ponudnikov storitev IKT.

2.2.3. Ocena in utemeljitev stroškovne učinkovitosti kontrol (razmerje „stroški kontrol ÷ vrednost z njimi povezanih upravljanih sredstev“) ter ocena pričakovane stopnje tveganja napake (ob plačilu in ob zaključku)

Upravljavski in kontrolni sistemi, kot jih določajo uredbe o evropskih nadzornih organih, se že izvajajo. Evropski nadzorni organi tesno sodelujejo s Službo Komisije za notranjo revizijo, da bi zagotovili izpolnjevanje ustreznih standardov na vseh področjih okvira notranje kontrole. Te ureditve se bodo uporabljale tudi v zvezi z vlogo evropskih nadzornih organov v skladu s tem predlogom. Poleg tega Evropski parlament vsako proračunsko leto po priporočilu Sveta vsakemu evropskemu nadzornemu organu podeli razrešnico za izvrševanje njegovega proračuna.

2.3. Ukrepi za preprečevanje goljufij in nepravilnosti

Navedite obstoječe ali načrtovane preprečevalne in zaščitne ukrepe, npr. iz strategije za boj proti goljufijam.

Za namene boja proti goljufijam, korupciji in drugim nezakonitim dejavnostim veljajo za evropske nadzorne organe brez kakršnih koli omejitev določbe Uredbe (EU, Euratom) št. 883/2013 Evropskega parlamenta in Sveta z dne 11. septembra 2013 o preiskavah, ki jih izvaja Evropski urad za boj proti goljufijam (OLAF).

Evropski nadzorni organi imajo posebej za to namenjeno strategijo boja proti goljufijam in akcijski načrt, ki temelji na njej. Okrepljeni ukrepi evropskih nadzornih organov na področju boja proti goljufijam bodo skladni s pravili in navodili iz finančne uredbe (ukrepi za boj proti goljufijam kot del dobrega finančnega poslovodenja), politiko urada OLAF za preprečevanje goljufij, določbami iz strategije Komisije na področju boja proti goljufijam (COM(2011) 376) in skupnega pristopa glede decentraliziranih agencij EU (julij 2012) ter s tem povezanim časovnim načrtom.

Poleg tega uredbe o ustanovitvi evropskih nadzornih organov in finančni predpisi zanje vsebujejo določbe o izvrševanju in nadzoru njihovega proračuna ter veljavna finančna pravila, vključno s pravili o preprečevanju goljufij in nepravilnosti.

3. OCENA FINANČNIH POSLEDIC PREDLOGA/POBUDE

3.1. Zadevni razdelki večletnega finančnega okvira in odhodkovne proračunske vrstice

Obstoječe proračunske vrstice

Po vrstnem redu razdelkov večletnega finančnega okvira in proračunskih vrstic

Razdelek večletnega finančnega okvira	Proračunska vrstica	Vrsta odhodkov	Prispevek			
	številka	dif./nedif. [52]	držav Efte [53]	držav kandidatk [54]	tretjih držav	po členu 21(2)(b) finančne uredbe

Zahtevane nove proračunske vrstice

Po vrstnem redu razdelkov večletnega finančnega okvira in proračunskih vrstic

Razdelek večletnega finančnega okvira	Proračunska vrstica	Vrsta odhodkov	Prispevek			
	številka	dif./nedif.	držav Efte	držav kandidatk	tretjih držav	po členu 21(2)(b) finančne uredbe

[52] Dif. = diferencirana sredstva / nedif. = nediferencirana sredstva.

[53] Efta: Evropsko združenje za prosto trgovino.

[54] Države kandidatke in po potrebi potencialne države kandidatke z Zahodnega Balkana.

3.2. Ocenjene posledice za odhodke

3.3. Povzetek ocenjenih posledic za odhodke

v mio. EUR (na tri decimalna mesta natančno)

Razdelek večletnega finančnega okvira	številka	Postavka

GD <..>			2020	2021	2022	2023	2024	2025	2026	2027	**SKUPAJ**
	obveznosti	(1)									
	plačila	(2)									
Odobritve za GD <.....> SKUPAJ	obveznosti										
	plačila										

Razdelek večletnega finančnega okvira		

v mio. EUR (na tri decimalna mesta natančno)

		2022	2023	2024	2025	2026	2027	**SKUPAJ**
GD <…….>								
• Človeški viri								
• Drugi upravni odhodki <>								
GD <…….> SKUPAJ	odobritve							

Odobritve iz RAZDELKA večletnega finančnega okvira **SKUPAJ**	(obveznosti skupaj = plačila skupaj)							

v mio. EUR (na tri decimalna mesta natančno) v stalnih cenah

		2022	**2023**	**2024**	**2025**	**2026**	**2027**	**SKUPAJ**
Odobritve iz RAZDELKA 1 večletnega finančnega okvira **SKUPAJ**	obveznosti							
	plačila							

3.3.1. Ocenjene posledice predloga za odobritve

☑ Za predlog/pobudo niso potrebne odobritve za poslovanje.

☐ Za predlog/pobudo so potrebne odobritve za poslovanje, kot je pojasnjeno v nadaljevanju:

odobritve za prevzem obveznosti v mio. EUR (na tri decimalna mesta natančno) v stalnih cenah

Cilji in realizacije			2022		2023		2024		2025		2026		2027		**SKUPAJ**	
	REALIZACIJE															
⇩	vrsta[55]	povprečni stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število realizacij skupaj	stroški realizacij skupaj
SPECIFIČNI CILJ št. 1[56] …																
–																
Seštevek za specifični cilj št. 1																
SPECIFIČNI CILJ št. 2 ...																
–																
Seštevek za specifični cilj št. 2																
STROŠKI SKUPAJ																

[55] Realizacije so dobavljeni proizvodi in opravljene storitve (npr. število financiranih izmenjav študentov, število kilometrov novozgrajenih cest …).

[56] Kakor je opisan v točki 1.4.2 „Specifični cilji …“.

3.3.2. Ocenjene posledice za človeške vire

3.3.2.1. Povzetek

☐ Za predlog/pobudo niso potrebne odobritve za upravne zadeve.

☑ Za predlog/pobudo so potrebne odobritve za upravne zadeve, kot je pojasnjeno v nadaljevanju:

v mio. EUR (na tri decimalna mesta natančno) v stalnih cenah

EBA, EIOPA, ESMA	2022	2023	2024	2025	2026	2027	**SKUPAJ**
Začasni uslužbenci (razredi AD)	1,188	2,381	2,381	2,381	2,381	2,381	13,093
Začasni uslužbenci (razredi AST)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Pogodbeni uslužbenci							
Napoteni nacionalni strokovnjaki							
SKUPAJ	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Potrebe po uslužbencih (EPDČ):

EBA, EIOPA, ESMA & EGP	2022	2023	2024	2025	2026	2027	**SKUPAJ**
Začasni uslužbenci (razredi AD) EBA = 5, EIOPA = 5, ESMA = 5	15	15	15	15	15	15	15
Začasni uslužbenci (razredi AST) EBA = 1, EIOPA = 1, ESMA = 1	3	3	3	3	3	3	3
Pogodbeni uslužbenci							
Napoteni nacionalni strokovnjaki							
SKUPAJ	**18**	**18**	**18**	**18**	**18**	**18**	**18**

3.3.2.2. Ocenjene potrebe po človeških virih za (matični) GD

☑ Za predlog/pobudo niso potrebni človeški viri.

☐ Za predlog/pobudo so potrebni človeški viri, kot je pojasnjeno v nadaljevanju:

ocena, izražena v celih številkah (ali na največ eno decimalno mesto natančno)

		2022	2023	2024	2025	2026	2027
• **Delovna mesta v skladu s kadrovskim načrtom (uradniki in začasni uslužbenci)**							
• **Zunanji sodelavci (v ekvivalentu polnega delovnega časa: EPDČ)**[57]							
XX 01 02 01 (PU, NNS, ZU iz splošnih sredstev)							
XX 01 02 02 (PU, LU, NNS, ZU in MSD na delegacijah)							
XX 01 04 ***yy***[58]	– na sedežu[59]						
	– na delegacijah						
XX 01 05 02 (PU, NNS, ZU za posredne raziskave)							
10 01 05 02 (PU, NNS, ZU za neposredne raziskave)							
Druge proračunske vrstice (navedite)							
SKUPAJ							

XX je zadevno področje ali naslov v proračunu.

Potrebe po človeških virih se krijejo z osebjem GD, ki je že dodeljeno za upravljanje ukrepa in/ali je bilo prerazporejeno znotraj GD, po potrebi skupaj z dodatnimi viri, ki se lahko pristojnemu GD dodelijo v okviru postopka letne dodelitve virov glede na proračunske omejitve.

Opis nalog:

Uradniki in začasni uslužbenci	
Zunanji sodelavci	

Opis izračuna stroškov za enote EPDČ mora biti vključen v oddelek 3 Priloge V.

[57] PU = pogodbeni uslužbenec; LU = lokalni uslužbenec; NNS = napoteni nacionalni strokovnjak; ZU = začasni uslužbenec; MSD = mladi strokovnjak na delegaciji.

[58] Dodatna zgornja meja za zunanje sodelavce v okviru odobritev za poslovanje (prej vrstice BA).

[59] Zlasti za strukturna sklada, Evropski kmetijski sklad za razvoj podeželja (EKSRP) in Evropski sklad za ribištvo (ESR).

3.3.3. Skladnost z veljavnim večletnim finančnim okvirom

☑ Predlog/pobuda je v skladu z veljavnim večletnim finančnim okvirom.

☐ Za predlog/pobudo je potrebna sprememba zadevnega razdelka večletnega finančnega okvira.

☐ Za predlog/pobudo je potrebna uporaba instrumenta prilagodljivosti ali sprememba večletnega finančnega okvira[60].

Pojasnite te zahteve ter navedite zadevne razdelke in proračunske vrstice ter ustrezne zneske. […]

3.3.4. Udeležba tretjih oseb pri financiranju

☐ V predlogu/pobudi ni načrtovano sofinanciranje tretjih oseb.

☑ V predlogu/pobudi je načrtovano sofinanciranje, kot je ocenjeno v nadaljevanju:

v mio. EUR (na tri decimalna mesta natančno)

EBA

	2022	2023	2024	2025	2026	2027	Skupaj
Stroški se bodo v celoti financirali z nadomestili, zaračunanimi nadzorovanim subjektom[61]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Sofinancirane odobritve SKUPAJ	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Skupaj
Stroški se bodo v celoti financirali z nadomestili, zaračunanimi nadzorovanim subjektom[62]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
Sofinancirane odobritve SKUPAJ	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

60 Glej člena 11 in 17 Uredbe Sveta (EU, Euratom) št. 1311/2013 o večletnem finančnem okviru za obdobje 2014–2020.

61 100 % skupnih predvidenih stroškov plus celotni prispevki delodajalca za pokojnine.

62 100 % skupnih predvidenih stroškov plus celotni prispevki delodajalca za pokojnine.

	2022	2023	2024	2025	2026	2027	Skupaj
Stroški se bodo v celoti financirali z nadomestili, zaračunanimi nadzorovanim subjektom[63]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Sofinancirane odobritve SKUPAJ	1,373	1,948	1,748	1,748	1,748	1,748	10,313

3.4. Ocenjene posledice za prihodke

☑ Predlog/pobuda nima finančnih posledic za prihodke.

☐ Predlog/pobuda ima finančne posledice, kot je pojasnjeno v nadaljevanju:

☐ za lastna sredstva,

☐ za druge prihodke.

☐ navedite, ali so prihodki dodeljeni za odhodkovne vrstice

v mio. EUR (na tri decimalna mesta natančno)

Prihodkovna proračunska vrstica	Odobritve na voljo za tekoče proračunsko leto	Posledice predloga/pobude[64]						
		Leto **N**	Leto **N+1**	Leto **N+2**	Leto **N+3**	Vstavite ustrezno število let glede na trajanje posledic (gl. točko 1.6)		
Člen …….								

Za razne namenske prejemke navedite zadevne odhodkovne proračunske vrstice.

[…]

Navedite metodo za izračun posledic za prihodke.

[…]

63 100 % skupnih predvidenih stroškov plus celotni prispevki delodajalca za pokojnine.

64 Pri tradicionalnih lastnih sredstvih (carine, prelevmani na sladkor) se navedejo neto zneski, tj. bruto zneski po odbitku 20 % stroškov pobiranja.

PRILOGA

Splošne predpostavke

Naslov I – Odhodki za zaposlene

Pri izračunu odhodkov za zaposlene na podlagi opredeljenih potreb po osebju, pojasnjenih spodaj, so bile uporabljene naslednje posebne predpostavke:

- stroški dodatnega osebja, zaposlenega leta 2022, so ocenjeni za 6 mesecev glede na predvideni čas, potreben za zaposlitev dodatnega osebja;
- povprečni letni stroški za začasnega uslužbenci znašajo 150 000 EUR, kar vključuje 25 000 EUR stroškov za službene prostore (zgradbe, IT itd.);
- korekcijska koeficienta, ki veljata za plače zaposlenih v Parizu (EBA in ESMA) in Frankfurtu (EIOPA), znašata 117,7 oziroma 99,4;
- pokojninski prispevki delodajalca za začasne uslužbence so temeljili na standardnih osnovnih plačah, vključenih v standardne povprečne letne stroške, tj. 95 660 EUR;
- dodatni začasni uslužbenci spadajo v razreda AD 5 in AST.

Naslov II – Odhodki za infrastrukturo in poslovanje

Stroški temeljijo na pomnožitvi števila zaposlenih z deležem v letu zaposlitve s standardnimi stroški za službene prostore, tj. 25 000 EUR.

Naslov III – Odhodki iz poslovanja

Stroški so ocenjeni na podlagi naslednjih predpostavk:

- stroški prevajanja znašajo 350 000 EUR na leto za vsak evropski nadzorni organ;
- enkratni stroški na področju IT v višini 500 000 EUR za vsak evropski nadzorni organ se plačajo v dveletnem obdobju 2022–2023 po načelu 50 : 50; letni stroški vzdrževanja po letu 2024 so ocenjeni na 50 000 EUR za vsak evropski nadzorni organ;
- letni stroški nadzora na kraju samem so ocenjeni na 200 000 EUR za vsak evropski nadzorni organ.

Zgoraj predstavljene ocene pomenijo naslednje stroške na letni ravni:

Razdelek večletnega finančnega okvira	Številka	

Stalne cene

EBA:			2022	2023	2024	2025	2026	2027	**SKUPAJ**
Naslov 1:	obveznosti	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	plačila	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Naslov 2:	obveznosti	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	plačila	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Naslov 3:	obveznosti	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	plačila	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
Odobritve za EBA SKUPAJ	obveznosti	= 1 + 1a + 3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	plačila	= 2 + 2a + 3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA:			2022	2023	2024	2025	2026	2027	**SKUPAJ**
Naslov 1:	obveznosti	(1)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	plačila	(2)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
Naslov 2:	obveznosti	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	plačila	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Naslov 3:	obveznosti	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	plačila	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000

Odobritve za EIOPA SKUPAJ	obveznosti	= 1 + 1a + 3a	1,305	1,811	1,611	1,611	1,611	1,611	9,560
	plačila	= 2 + 2a + 3b	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA:			2022	2023	2024	2025	2026	2027	**SKUPAJ**
Naslov 1:	obveznosti	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	plačila	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Naslov 2:	obveznosti	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	plačila	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Naslov 3:	obveznosti	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	plačila	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
Odobritve za ESMA SKUPAJ	obveznosti	= 1 + 1a + 3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	plačila	= 2 + 2a + 3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

Za predlog so potrebne odobritve za poslovanje, kot je pojasnjeno v nadaljevanju:

Odobritve za prevzem obveznosti v mio. EUR (na tri decimalna mesta natančno) v stalnih cenah

EBA

Cilji in realizacije			2022		2023		2024		2025		2026		2027			
	REALIZACIJE															
⇩	vrsta[65]	povprečni stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število realizacij skupaj	stroški realizacij skupaj
SPECIFIČNI CILJ št. 1[66] Neposredni nadzor nad ključnimi tretjimi ponudniki storitev IKT																
–				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Seštevek za specifični cilj št. 1																
SPECIFIČNI CILJ št. 2 ...																
–																
Seštevek za specifični cilj št. 2																
STROŠKI SKUPAJ				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

EIOPA

Cilji in realizacije			2022		2023		2024		2025		2026		2027			
	REALIZACIJE															
⇩	vrsta[67]	povprečni stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število realizacij skupaj	stroški realizacij skupaj
SPECIFIČNI CILJ št. 1[68] Neposredni nadzor nad ključnimi tretjimi ponudniki storitev IKT																

[65] Realizacije so dobavljeni proizvodi in opravljene storitve (npr. število financiranih izmenjav študentov, število kilometrov novozgrajenih cest …).

[66] Kakor je opisan v točki 1.4.2 „Specifični cilji …“.

[67] Realizacije so dobavljeni proizvodi in opravljene storitve (npr. število financiranih izmenjav študentov, število kilometrov novozgrajenih cest …).

[68] Kakor je opisan v točki 1.4.2 „Specifični cilji …“.

–				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Seštevek za specifični cilj št. 1																
SPECIFIČNI CILJ št. 2 ...																
–																
Seštevek za specifični cilj št. 2																
STROŠKI SKUPAJ				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

ESMA

Cilji in realizacije			2022		2023		2024		2025		2026		2027			
	REALIZACIJE															
⇩	vrsta[69]	povprečni stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število realizacij skupaj	stroški realizacij skupaj
SPECIFIČNI CILJ št. 1[70] Neposredni nadzor nad ključnimi tretjimi ponudniki storitev IKT																
–				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Seštevek za specifični cilj št. 1																
SPECIFIČNI CILJ št. 2 ...																
–																
Seštevek za specifični cilj št. 2																
STROŠKI SKUPAJ				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

[69] Realizacije so dobavljeni proizvodi in opravljene storitve (npr. število financiranih izmenjav študentov, število kilometrov novozgrajenih cest …).

[70] Kakor je opisan v točki 1.4.2 „Specifični cilji …“.

Dejavnosti nadzora se v celoti financirajo z nadomestili, zaračunanimi nadzorovanim subjektom, kot sledi:

EBA

	2022	2023	2024	2025	2026	2027	Skupaj
Stroški se bodo v celoti financirali z nadomestili, zaračunanimi nadzorovanim subjektom[71]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Sofinancirane odobritve SKUPAJ	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Skupaj
Stroški se bodo v celoti financirali z nadomestili, zaračunanimi nadzorovanim subjektom[72]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
Sofinancirane odobritve SKUPAJ	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022	2023	2024	2025	2026	2027	Skupaj
Stroški se bodo v celoti financirali z nadomestili, zaračunanimi nadzorovanim subjektom[73]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Sofinancirane odobritve SKUPAJ	1,373	1,948	1,748	1,748	1,748	1,748	10,313

[71] 100 % skupnih predvidenih stroškov plus celotni prispevki delodajalca za pokojnine.
[72] 100 % skupnih predvidenih stroškov plus celotni prispevki delodajalca za pokojnine.
[73] 100 % skupnih predvidenih stroškov plus celotni prispevki delodajalca za pokojnine.

SPECIFIČNE INFORMACIJE

Pooblastila za neposredni nadzor

Uvodoma je treba spomniti, da bi morali subjekti, ki jih ESMA neposredno nadzoruje, temu organu plačevati nadomestila (enkratni stroški za registracijo in redni stroški za stalni nadzor). To velja za bonitetne agencije (glej Delegirano uredbo Komisije (EU) št. 272/2012) in repozitorije sklenjenih poslov (Delegirana uredba Komisije (EU) št. 1003/2013).

V skladu s tem zakonodajnim predlogom bodo evropskim nadzornim organom zaupane nove naloge, katerih namen je spodbujati konvergenco nadzornih pristopov k tveganjem tretjih oseb na področju IKT v finančnem sektorju, tako da se vzpostavi okvir nadzora Unije za ključne tretje ponudnike storitev IKT.

Okvir nadzora, ki ga predvideva ta predlog, temelji na obstoječi institucionalni arhitekturi na področju finančnih storitev, pri čemer Skupni odbor evropskih nadzornih organov zagotavlja medsektorsko usklajevanje v zvezi z vsemi zadevami v zvezi s tveganji na področju IKT v skladu s svojimi nalogami na področju kibernetske varnosti, pri tem pa ga podpira pododbor (nadzorniški forum), ki izvaja pripravljalno delo za posamezne odločitve in skupna priporočila, naslovljena na ključne tretje ponudnike storitev IKT.

S tem okvirom bodo evropski nadzorni organi, ki bodo imenovani za glavne nadzornike za vsakega ključnega tretjega ponudnika storitev IKT, prejeli pooblastila za zagotovitev, da se ponudniki tehnoloških storitev, ki imajo ključno vlogo pri delovanju finančnega sektorja, ustrezno spremljajo na vseevropski ravni. Nadzorne naloge so določene v predlogu in dodatno pojasnjene v obrazložitvenem memorandumu. Vključujejo pravice za zahtevanje vseh ustreznih informacij in dokumentacije za izvajanje splošnih preiskav in inšpekcijskih pregledov, pošiljanje priporočil in naknadno predložitev poročil o sprejetih ukrepih ali popravnih ukrepih, ki jih je izvedel naslovnik navedenih priporočil.

Evropski nadzorni organi bodo za izvajanje novih nalog, predvidenih s tem predlogom, najeli dodatno osebje, ki je specializirano za tveganja na področju IKT in se osredotoča na ocenjevanje odvisnosti od tretjih oseb.

Kadrovske potrebe se lahko ocenijo na šest redno zaposlenih z EPDČ za vsak organ (pet delovnih mest AD in eno delovno mesto AST za podporo uslužbencem razreda AD). Evropski nadzorni organi bodo imeli tudi dodatne stroške na področju IT, ocenjene na 500 000 EUR (enkratni stroški), ter 50 000 EUR letno za vsakega od treh evropskih nadzornih organov za stroške vzdrževanja. Pomemben element pri izpolnjevanju novih nalog so naloge za izvajanje inšpekcijskih pregledov in revizij na kraju samem, ki jih je mogoče oceniti na 200 000 EUR letno za vsak evropski nadzorni organ. Stroški prevajanja za različne dokumente, ki bi jih evropski nadzorni organi prejeli od ključnih tretjih ponudnikov storitev IKT, so prav tako vključeni v vrstico o operativnih stroških in znašajo 350 000 EUR letno.

Vsi zgoraj navedeni upravni stroški se bodo v celoti financirali z letnimi nadomestili, ki jih bodo evropski nadzorni organi zaračunavali ključnim tretjim ponudnikom storitev IKT (brez vpliva na proračun EU).