Svet
Evropske unije

Bruselj, 24. september 2020
(OR. en)

Medinstitucionalna zadeva:
2020/0268 (COD)

11052/20
ADD 2

EF 229
ECOFIN 847
TELECOM 160
CYBER 169
IA 62
CODEC 872

SPREMNI DOPIS

Pošiljatelj:	za generalno sekretarko Evropske komisije: direktor Jordi AYET PUIGARNAU
Datum prejema:	24. september 2020
Prejemnik:	generalni sekretar Sveta Evropske unije Jeppe TRANHOLM-MIKKELSEN
Št. dok. Kom.:	SWD(2020) 204 final
Zadeva:	DELOVNI DOKUMENT SLUŽB KOMISIJE POVZETEK POROČILA O OCENI UČINKA Spremni dokument k predlogu direktive Evropskega parlamenta in Sveta o spremembi direktiv 2006/43/ES, 2009/65/ES, 2009/138/EU, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 in (EU) 2016/2341

Delegacije prejmejo priloženi dokument SWD(2020) 204 final.

Priloga: SWD(2020) 204 final

EVROPSKA
KOMISIJA

Bruselj, 24.9.2020
SWD(2020) 204 final

NOTE
This language version reflects the corrections done to the original EN version retransmitted under SWD(2020) 204 final/2 of 16.10.2020.

DELOVNI DOKUMENT SLUŽB KOMISIJE

POVZETEK POROČILA O OCENI UČINKA

Spremni dokument

k predlogu direktive Evropskega parlamenta in Sveta

o spremembi direktiv 2006/43/ES, 2009/65/ES, 2009/138/EU, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 in (EU) 2016/2341

{COM(2020) 596 final} - {SEC(2020) 309 final} - {SWD(2020) 203 final}

Povzetek

Ocena učinka o predlogu uredbe o digitalni operativni odpornosti v finančnem sektorju

A. Nujnost ukrepanja

Zakaj? V čem je težava?

Finančni sektor se močno zanaša na informacijske in komunikacijske tehnologije (IKT). Trenutna pandemija COVID-19 bo to verjetno še stopnjevala glede na prednosti zagotavljanja stalnega oddaljenega dostopa do finančnih storitev. Vendar zanašanje na digitalne tehnologije prinaša tudi skrbi; podjetja morajo biti sposobna prenesti morebitne motnje na področju IKT, da se lahko obravnavajo digitalni incidenti in grožnje ter ohranjajo storitve. Čeprav ranljivosti, ki izhajajo iz odvisnosti od IKT, veljajo za vse gospodarske sektorje, so v medsebojno močno povezanem finančnem sektorju, ki uporablja čezmejne ključne storitve, od katerih je odvisno realno gospodarstvo, še posebno izrazite zaradi (1) globoke in široke uporabe IKT ter (2) možnosti, da se učinki operativnega incidenta v enem finančnem podjetju ali finančnem podsektorju hitro razširijo na druga podjetja ali dele finančnega sektorja in nazadnje na preostalo gospodarstvo.

Čeprav je finančni sektor zelo napredoval pri tržnem in regulativnem povezovanju in uspešno deluje na podlagi harmoniziranih pravil – enotna pravila EU –, je bil odziv EU na povečane potrebe po operativni odpornosti na horizontalni in sektorski ravni bodisi:

- odziv na podlagi minimalne uskladitve, ki dopušča nacionalno razlago in razdrobljenost na enotnem trgu, bodisi
- preveč splošen in omejen odziv, ki v različni meri obravnava splošno operativno tveganje, pri čemer delno ureja nekatere komponente digitalne operativne *odpornosti* (npr. upravljanje tveganj na področju IKT, poročanje o incidentih in tveganja tretjih oseb na področju IKT), medtem ko drugih ne vključuje (testiranje).

EU pri svojem posredovanju doslej ni obravnavala operativnega tveganja na način, ki ustreza potrebam finančnih podjetij, da se odzovejo na ranljivosti na področju IKT in okrevajo po njih, niti finančnim nadzornikom ne zagotavlja orodij za izpolnjevanje njihovih nalog za zajezitev finančne nestabilnosti, ki izhaja iz teh ranljivosti na področju IKT.

Trenutne vrzeli in nedoslednosti so privedle do vse večjega števila neusklajenih nacionalnih pobud (npr. v zvezi s testiranjem) in nadzornih pristopov (npr. v zvezi z odvisnostmi od tretjih oseb na področju IKT), ki vodijo do prekrivanj, podvajanj zahtev ter visokih upravnih stroškov in stroškov izpolnjevanja obveznosti za čezmejna finančna podjetja ali do neodkrivanja in neobravnavanja tveganj na področju IKT. Stabilnost in celovitost finančnega sektorja nista zagotovljeni, enotni trg finančnih storitev pa ostaja razdrobljen, zaradi česar so potrošniki in vlagatelji slabše zaščiteni.

Kaj naj bi prinesla ta pobuda?

Splošni cilj je okrepiti digitalno operativno odpornost finančnega sektorja EU z racionalizacijo in nadgradnjo obstoječe finančne zakonodaje EU ter uvajanjem novih zahtev v primeru vrzeli, kar je namenjeno:

- izboljšanju upravljanja tveganj na področju IKT, ki ga izvajajo finančna podjetja;
- okrepitvi znanja nadzornih organov o grožnjah in incidentih;
- izboljšanju testiranja, ki ga izvajajo finančna podjetja za svoje sisteme IKT, ter
- boljšemu nadzoru nad tveganji, ki izhajajo iz odvisnosti finančnih podjetij od tretjih ponudnikov storitev IKT.

Natančneje, predlog bi ustvaril skladnejše in doslednejše mehanizme poročanja o incidentih ter tako zmanjšal upravna bremena za finančne institucije in okrepil učinkovitost nadzora.

Kakšna je dodana vrednost ukrepanja na ravni EU?

Enotni trg EU za finančne storitve ureja obsežen sklop pravil, določenih na ravni EU, ki finančnim podjetjem z dovoljenjem v eni državi članici na podlagi dovoljenja EU za čezmejno opravljanje dejavnosti omogočajo izvajanje storitev na celotnem enotnem trgu. Posledično pravila na nacionalni ravni ne bi bila učinkovit način za krepitev operativne odpornosti finančnih podjetij, ki uporabljajo dovoljenje za čezmejno opravljanje dejavnosti. Poleg tega enotna pravila EU zaradi finančne krize vsebujejo zelo podrobna in predpisujoča pravila, ki obravnavajo bolj „tradicionalna“ tveganja, kot so kreditno, tržno in likvidnostno tveganje ter tveganje nasprotne stranke. Obstoječe določbe o operativnem tveganju ostajajo splošne. Krepitev digitalne operativne odpornosti zahteva prilagoditve določb o operativnih tveganjih, ki so že opredeljene na ravni EU in jih je zato mogoče posodobiti in dopolniti le na ravni EU.

B. Rešitve

Katere zakonodajne in nezakonodajne možnosti politike so se upoštevale? Ali ima katera od njih prednost? Zakaj?

Ocena učinka je poleg osnovnega scenarija neukrepanja v zvezi z zakonodajo EU o finančnih storitvah obravnavala tri možnosti. Natančneje:

- **„brez ukrepanja“:** sedanje različne določbe EU o finančnih storitvah, deloma tudi direktiva o kibernetski varnosti (NIS), in obstoječe ali prihodnje nacionalne ureditve bi še naprej določale pravila o operativni odpornosti;
- **možnost 1 – krepitev kapitalskih blažilnikov:** uvedel bi se dodatni kapitalski blažilnik za povečanje zmožnosti finančnih podjetij, da pokrijejo izgube, ki bi lahko nastale zaradi neobstoja operativne odpornosti;
- **možnost 2 – akt o digitalni operativni odpornosti na področju finančnih storitev:** s tem bi se uvedel celovit okvir na ravni EU, ki bi določal pravila o digitalni operativni odpornosti za vse regulirane finančne institucije in bi:
  - celoviteje obravnaval tveganja na področju IKT;
  - finančnim nadzornikom omogočil dostop do informacij o incidentih, povezanih z IKT;
  - zagotovil, da finančna podjetja ocenijo učinkovitost svojih varnostnih ukrepov in ukrepov za odpornost ter prepoznajo ranljivosti na področju IKT;
  - okrepil pravila zunanjega izvajanja, ki urejajo posreden nadzor nad tretjimi ponudniki storitev IKT;
  - omogočil neposreden nadzor nad dejavnostmi tretjih ponudnikov storitev IKT, kadar svoje storitve zagotavljajo finančnim podjetjem, in
  - poleg tega spodbudil izmenjavo obveščevalnih podatkov o grožnjah v finančnem sektorju;
- **možnost 3 – akt o odpornosti v kombinaciji s centraliziranim nadzorom nad ključnimi tretjimi ponudniki:** poleg uvedbe akta o operativni odpornosti (možnost 2) bi bil ustanovljen nov organ za nadzor nad ključnimi storitvami IKT, ki jih tretji ponudniki storitev IKT zagotavljajo finančnim podjetjem. Prav tako bi jasneje ločil finančni sektor od področja uporabe direktive o kibernetski varnosti.

Možnost 2 je prednostna možnost. V primerjavi z drugima možnostma doseže večino ciljev pobude ter hkrati upošteva merila učinkovitosti in skladnosti. Ta možnost uživa tudi največjo podporo zainteresiranih strani.

Kdo podpira katero možnost?

Večina zainteresiranih strani (zasebnih, javnih) se strinja, da so potrebni ukrepi EU za boljše varstvo operativne odpornosti finančnih podjetij. Veliko jih tudi meni, da je treba z ukrepi EU odpraviti regulativna bremena, ki izhajajo iz dejstva, da za finančna podjetja veljajo podvojena in nedosledna pravila iz direktive o kibernetski varnosti, zakonodaje EU o finančnih storitvah in nacionalnih ureditev (npr. glede poročanja o incidentih). Zato le malo zainteresiranih strani podpira možnost neukrepanja. Le malo zainteresiranih strani vidi koristi v zagotavljanju operativne odpornosti s povečanimi kapitalskimi blažilniki (možnost 1). Vendar je to tradicionalni pristop k operativnemu tveganju, zlasti v bančništvu, in ga kot takega obravnavajo na primer mednarodni organi za določanje standardov. Vrsta kvalitativnih ukrepov, določenih v možnosti 2, ki bi racionalizirali in nadgradili finančno zakonodajo EU in uvedli nove zahteve v primeru vrzeli, hkrati pa ohranili povezave s horizontalno direktivo o kibernetski varnosti, uživa široko podporo zainteresiranih strani, ki so sodelovale pri javnem posvetovanju. Nekatere zainteresirane strani (zlasti javne) vidijo koristi v okrepljenem nadzoru nad tretjimi ponudniki storitev IKT iz možnosti 3, vendar imata ustanovitev novega organa EU v ta namen in popolna ločitev od okvira direktive o kibernetski varnosti le omejeno podporo zainteresiranih strani.

C. Učinki prednostne možnosti

Kakšne so koristi prednostne možnosti (če obstaja, sicer glavnih možnosti)?

Možnost 2 bi obravnavala **tveganja na področju IKT** v finančnem sektorju s povečanjem zmogljivosti finančnih institucij, da vzdržijo incidente na področju IKT. S tem bi se zmanjšalo tveganje, da bi se kibernetski incident hitro razširil na finančne trge. Čeprav je težko oceniti stroške operativnih incidentov v finančnem sektorju (vsi incidenti niso prijavljeni; obseg stroškov ni točen), ocene industrije kažejo, da bi se stroški finančnega sektorja EU lahko gibali med 2 in 27 milijard EUR na leto. Prednostna možnost bi znižala te neposredne stroške in morebitne širše učinke, ki jih večji kibernetski incidenti lahko imajo na finančno stabilnost. Odprava prekrivajočih se **zahtev o poročanju** bi zmanjšala upravna bremena. Na primer, pri nekaterih največjih bankah lahko s tem povezani prihranki znašajo od 40 do 100 milijonov EUR na leto. Neposredno poročanje bi tudi okrepilo znanje nadzornikov o incidentih na področju IKT. **Usklajeno testiranje** bi izboljšalo odkrivanje neznanih ranljivosti in tveganj. Prav tako bi znižalo stroške, zlasti za čezmejna podjetja. Za 44 največjih čezmejnih bank bi se celotne pričakovane koristi skupnega pristopa k testiranju na primer gibale med 11 in 88 milijoni EUR. Z uvedbo skladnih pravil o upravljanju tveganj **tretjih ponudnikov storitev IKT** bi imela finančna podjetja večji nadzor nad tem, kako tretji ponudniki storitev spoštujejo regulativni okvir, kar bi pomagalo nadzornikom. Nadzor nad tretjimi ponudniki storitev IKT bi prinesel tudi bonitetne koristi. Prednostna možnost pomeni širše družbene koristi, ki

izhajajo iz odpornejšega operativnega okolja za vse udeležence na finančnem trgu ter okrepljene zaščite potrošnikov in vlagateljev.

Kakšni so stroški prednostne možnosti (če obstaja, sicer glavnih možnosti)?

Prednostna možnost bi privedla do enkratnih in ponavljajočih se stroškov. Enkratni stroški so posledica naložb v informacijske sisteme in jih je zaradi različnega stanja obstoječih sistemov podjetij težko količinsko opredeliti. Ker ni bilo regulativnega posredovanja, so nekatera finančna podjetja že znatno vlagala v sisteme IKT. To pomeni, da bo stopnja izvajanja ukrepov iz tega predloga za večja finančna podjetja verjetno nizka. Za manjša podjetja naj bi bili tudi stroški nižji, saj bi zanje veljali manj strogi ukrepi, sorazmerni z njihovim manjšim tveganjem. Kar zadeva testiranje, so evropski nadzorni organi ocenili, da se stroški, povezani s penetracijskim testiranjem na podlagi analize groženj, gibljejo med 0,1 % in 0,3 % celotnega proračuna zadevnih podjetij za IKT. Stroški, povezani s poročanjem o incidentih, bi se drastično znižali, saj ne bi prihajalo do prekrivanj s poročanjem na podlagi direktive o kibernetski varnosti. Tudi nadzorniki bodo imeli nekaj stroškov zaradi dodatnih nalog, ki bi jih prevzeli. Na primer, za nadzornike, ki sodelujejo pri neposrednem nadzoru nad tretjimi ponudniki storitev IKT, je mogoče pričakovati povečanje EPDČ v razponu od 1 do 5 EPDČ za vodilni organ in približno 0,25 EPDČ za sodelujoče organe.

Kakšen bo vpliv na podjetja, MSP ter mikro podjetja?

Prednostna možnost bi zajela vsa finančna podjetja, da bi se povečala operativna odpornost celotnega sektorja. To široko področje uporabe je pomembno zaradi medsebojno povezane narave finančnega sektorja in s tem povezane potrebe po ustrezni splošni operativni odpornosti. Vendar bi pri opredelitvi temeljnih zahtev na glavnih področjih ukrepanja med različnimi podsektorji in znotraj vsakega podsektorja veljalo načelo sorazmernosti. Med drugim bi se upoštevale razlike v poslovnih modelih, velikosti, profilu tveganja, sistemskem pomenu itd. Ukrepi za poročanje o incidentih in testiranje bi bili na primer manj strogi za manjša finančna podjetja.

Ali bo prišlo do znatnih učinkov na nacionalne proračune in uprave?

Ne. Dodatni nadzor lahko, kot je prikazano zgoraj, zahteva omejeno stopnjo dodatnih nadzornih virov, katerih stroške lahko v celoti ali delno (v primeru nadomestil za nadzor) nosijo javni proračuni.

Ali bo prišlo do drugih pomembnih učinkov?

Socialno-ekonomske posledice pandemije COVID-19 dokazujejo ključni pomen digitalnih finančnih trgov in njihove operativne odpornosti. Prednostna možnost bi bila dobra podlaga za izkoriščanje digitalne preobrazbe z zagotavljanjem, da je enotni trg finančnih storitev, vključno z bančništvom in unijo kapitalskih trgov, operativno odporen na podlagi skupnih pravil in zahtev, ki stremijo k varnosti, zmogljivosti, stabilnosti in enakim konkurenčnim pogojem. S tem se bo tudi okrepil vodilni položaj Evrope na svetovnem finančnem in digitalnem področju, kar je cilj, ki si ga je Komisija zastavila v sporočilu z naslovom „Oblikovanje digitalne prihodnosti Evrope“.

D. Spremljanje

Kdaj se bo politika pregledala?

Prva ocena se izvede tri leta po začetku veljavnosti pravnega akta. Komisija bi Evropskemu parlamentu in Svetu predložila poročilo o pregledu. Pregled bi lahko po potrebi spremljala javna posvetovanja, študije, strokovne razprave, ankete in delavnice.