Rada
Európskej únie

V Bruseli 24. septembra 2020
(OR. en)

11052/20
ADD 2

Medziinštitucionálny spis:
2020/0268(COD)

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

SPRIEVODNÁ POZNÁMKA

Od:	Martine DEPREZOVÁ, riaditeľka, v zastúpení generálnej tajomníčky Európskej komisie
Dátum doručenia:	24. septembra 2020
Komu:	Jeppe TRANHOLM-MIKKELSEN, generálny tajomník Rady Európskej únie
Č. dok. Kom.:	SWD(2020) 204 final
Predmet:	PRACOVNÝ DOKUMENT ÚTVAROV KOMISIE ZHRNUTIE SPRÁVY O POSÚDENÍ VPLYVU Sprievodný dokument Návrh SMERNICA EURÓPSKEHO PARLAMENTU A RADY, ktorou sa menia smernice 2006/43/ES, 2009/65/ES, 2009/138/ES, 2011/61/EÚ, 2013/36/EÚ, 2014/65/EÚ, (EÚ) 2015/2366 a (EÚ) 2016/2341

Delegáciám v prílohe zasielame dokument SWD(2020) 204 final.

Príloha: SWD(2020) 204 final

EURÓPSKA
KOMISIA

V Bruseli 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

PRACOVNÝ DOKUMENT ÚTVAROV KOMISIE

ZHRNUTIE SPRÁVY O POSÚDENÍ VPLYVU

Sprievodný dokument

Návrh
SMERNICA EURÓPSKEHO PARLAMENTU A RADY,

ktorou sa menia smernice 2006/43/ES, 2009/65/ES, 2009/138/ES, 2011/61/EÚ, 2013/36/EÚ, 2014/65/EÚ, (EÚ) 2015/2366 a (EÚ) 2016/2341

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

Súhrnný prehľad

Posúdenie vplyvu návrhu nariadenia o digitálnej prevádzkovej odolnosti vo finančnom sektore

A. Potreba konať

Prečo? Aký problém sa rieši?

Finančný sektor vo veľkej miere využíva informačné a komunikačné technológie (IKT). Súčasná pandémia ochorenia COVID-19 tento vývoj pravdepodobne urýchli vzhľadom na výhody vyplývajúce zo zabezpečenia nepretržitého vzdialeného prístupu k finančným službám. Spoliehanie sa na digitálne technológie však prináša určité obavy; spoločnosti musia byť schopné čeliť potenciálnym narušeniam v oblasti IKT, aby sa digitálne incidenty a hrozby riešili a služby zostali zachované. V úzko prepojenom finančnom sektore, ktorý poskytuje dôležité cezhraničné služby, od ktorých závisí reálna ekonomika, sú zraniteľnosti vyplývajúce zo závislosti od IKT, a to platí pre všetky hospodárske odvetvia, obzvlášť výrazné z dôvodu 1. rozsiahleho a intenzívneho používania IKT a 2. možnosti rýchleho šírenia vplyvov prevádzkového incidentu v jednej finančnej spoločnosti alebo v jednom finančnom subsektore na iné spoločnosti alebo časti finančného sektora a v konečnom dôsledku na ostatné odvetvia hospodárstva.

Napriek tomu, že finančný sektor je veľmi vyspelý, pokiaľ ide o jeho trhovú a regulačnú integráciu, a využíva jednotný súbor harmonizovaných pravidiel – jednotný súbor pravidiel EÚ –, bola reakcia EÚ na zvýšenú potrebu prevádzkovej odolnosti na horizontálnej a odvetvovej úrovni buď:

- založená na minimálnej harmonizácii, čím vznikol priestor na vnútroštátny výklad a fragmentáciu na jednotnom trhu, alebo
- príliš všeobecná a s obmedzeným uplatnením, pričom sa v rôznom rozsahu zaoberala celkovým operačným rizikom, čiastočne regulovala niektoré prvky digitálnej prevádzkovej *odolnosti* (napr. riadenie IKT rizík, nahlasovanie incidentov a IKT riziká tretích strán), zatiaľ čo iné opomenula (testovanie).

Intervencia EÚ sa doteraz nezaoberala operačným rizikom takým spôsobom, ktorý by zodpovedal potrebám finančných spoločností čeliť zraniteľnostiam IKT, reagovať na ne a zotaviť sa z nich, ani neposkytuje orgánom finančného dohľadu nástroje na plnenie ich mandátu zmierniť finančnú nestabilitu vyplývajúcu z týchto zraniteľností IKT.

Súčasné nedostatky a nezrovnalosti viedli k rozšíreniu nekoordinovaných vnútroštátnych iniciatív (napr. pokiaľ ide o testovanie) a prístupov v oblasti dohľadu (napr. k závislosti od IKT tretích strán), čo sa premieta buď do prekrývania a duplicity požiadaviek a vysokých administratívnych nákladov a nákladov na dodržiavanie predpisov, ktoré vynakladajú cezhraničné finančné spoločnosti, alebo do stále neodhalených a neriešených IKT rizík. Celkovo nie je zaručená stabilita a integrita finančného sektora a jednotný trh s finančným službami ostáva roztrieštený, čo má za následok oslabenie ochrany spotrebiteľov a investorov.

Čo sa od tejto iniciatívy očakáva?

Celkovým cieľom je posilnenie digitálnej prevádzkovej odolnosti finančného sektora EÚ zefektívnením a modernizáciou súčasných finančných právnych predpisov EÚ a zavedením nových požiadaviek v oblastiach, kde existujú rozdiely, so zameraním na:

- zlepšenie riadenia IKT rizík finančnými spoločnosťami;
- zlepšenie znalostí orgánov dohľadu o hrozbách a incidentoch;
- zlepšenie testovania vlastných IKT systémov finančnými spoločnosťami a
- lepší dohľad nad rizikami vyplývajúcimi zo závislosti finančných spoločností od externých poskytovateľov IKT.

Konkrétnejšie by tento návrh vytvoril koherentnejšie a konzistentnejšie mechanizmy nahlasovania incidentov, čím by znížil administratívnu záťaž finančných inštitúcií a posilnil efektívnosť dohľadu.

Aká je pridaná hodnota opatrení na úrovni EÚ?

Jednotný trh EÚ s finančnými službami sa riadi veľkým množstvom pravidiel stanovených na úrovni EÚ, ktoré umožňujú finančným spoločnostiam s oprávnením na činnosť v jednom členskom štáte poskytovať služby v rámci celého jednotného trhu vďaka povoleniu EÚ. Preto by pravidlá na vnútroštátnej úrovni neboli účinným nástrojom na posilnenie prevádzkovej odolnosti finančných spoločností, ktoré využívajú toto povolenie. Okrem toho jednotný súbor pravidiel EÚ obsahuje v dôsledku finančnej krízy veľmi detailné a normatívne pravidlá zamerané na „tradičnejšie“ riziká, napríklad úverové riziko, trhové riziko, riziko protistrany a riziko likvidity. Existujúce ustanovenia o operačnom riziku ostávajú všeobecné. Posilnenie digitálnej prevádzkovej odolnosti si vyžaduje úpravu ustanovení o operačných rizikách, ktoré sú už definované na úrovni EÚ, a preto môžu byť zlepšené a doplnené len na úrovni EÚ.

B. Riešenia

Aké legislatívne a nelegislatívne možnosti politiky sa zvažovali? Je niektorá z možností uprednostňovaná? Prečo?

V posúdení vplyvu sa okrem základného scenára neprijať žiadne opatrenia, pokiaľ ide o právne predpisy EÚ v oblasti finančných služieb, zvažovali tri možnosti. Konkrétnejšie:

- „**Nezasahovať**“: pravidlá o prevádzkovej odolnosti by boli naďalej stanovené súčasným rozmanitým súborom ustanovení právnych predpisov EÚ o finančných službách, čiastočne smernicou NIS a existujúcimi alebo budúcimi vnútroštátnymi režimami;
- **Možnosť 1 – posilnenie kapitálového vankúša**: zaviedol by sa ďalší kapitálový vankúš na zvýšenie schopnosti finančných spoločností pokryť straty, ktoré by mohli vzniknúť z dôvodu nedostatočnej prevádzkovej odolnosti;
- **Možnosť 2 – akt o digitálnej prevádzkovej odolnosti finančných služieb**: tým by sa zaviedol komplexný rámec na úrovni EÚ, ktorým by sa stanovili pravidlá digitálnej prevádzkovej odolnosti pre všetky regulované finančné inštitúcie a ktorý by
  - sa komplexnejšie zaoberal IKT rizikami;
  - umožňoval orgánom finančného dohľadu prístup k informáciám o incidentoch súvisiacich s IKT;
  - zaistil, že finančné spoločnosti posúdia účinnosť svojich opatrení v oblasti predchádzania a odolnosti a identifikujú zraniteľnosti IKT;
  - posilnil pravidlá využívania externých zdrojov upravujúce nepriamy dohľad nad externými poskytovateľmi IKT;
  - umožnil priamy dohľad nad činnosťami externých poskytovateľov IKT, pri poskytovaní ich služieb finančným spoločnostiam a
  - okrem toho by podnietil výmenu spravodajských informácií o hrozbách vo finančnom sektore.
- **Možnosť 3 – akt o odolnosti v kombinácii s centralizovaným dohľadom nad externými poskytovateľmi kritických IKT služieb**: okrem aktu o prevádzkovej odolnosti (možnosť 2) by bol vytvorený nový orgán dohľadu nad externými poskytovateľmi kritických IKT služieb finančným spoločnostiam. Zároveň by jasnejšie vyčlenil finančný sektor z rozsahu pôsobnosti smernice NIS.

Uprednostňuje sa možnosť 2. V porovnaní s ostatnými možnosťami sa touto možnosťou dosiahne najviac cieľov danej iniciatívy pri zohľadnení kritérií efektívnosti a koherentnosti. Táto možnosť má zároveň najväčšiu podporu medzi zainteresovanými stranami.

Kto podporuje ktorú možnosť?

Väčšina zainteresovaných strán (zo súkromného a verejného sektora) súhlasí, že na lepšie zabezpečenie prevádzkovej odolnosti finančných spoločností sú potrebné opatrenia na úrovni EÚ. Mnohí sa takisto domnievajú, že opatrenia na úrovni EÚ sú potrebné na riešenie regulačnej záťaže, ktorá je spôsobená duplicitnými a nejednotnými pravidlami pre finančné spoločnosti stanovenými v smernici NIS, právnych predpisoch EÚ o finančných službách a vo vnútroštátnych režimoch (napr. pokiaľ ide o nahlasovanie incidentov). V súlade s tým niekoľko zainteresovaných strán podporuje možnosť nezasahovať. Niekoľko zainteresovaných strán vidí výhodu v zabezpečení prevádzkovej odolnosti prostredníctvom väčšieho kapitálového vankúša (možnosť 1). To je však tradičný prístup k operačnému riziku, najmä v bankovníctve, a za taký ho považujú napr. subjekty, ktoré stanovujú medzinárodné normy. Typ kvalitatívnych opatrení stanovených v možnosti 2, ktoré by zefektívnili a zmodernizovali finančné právne predpisy EÚ a zaviedli nové požiadavky v oblastiach, kde existujú rozdiely, a zároveň by zachovali prepojenia na horizontálnu smernicu NIS, získava širokú podporu zainteresovaných strán, ktoré sa zúčastnili verejnej konzultácie. Hoci niektoré zainteresované strany (najmä z verejného sektora) vidia výhodu v posilnení dohľadu nad externými poskytovateľmi IKT podľa možnosti 3, vytvorenie nového orgánu EÚ na tento účel má len obmedzenú podporu medzi zainteresovanými stranami, rovnako ako ucelenejšia odluka od rámca NIS.

C. Vplyvy uprednostňovanej možnosti

Aké sú výhody uprednostňovanej možnosti (prípadne hlavných možností, ak sa žiadna konkrétna možnosť neuprednostňuje)?

Možnosť 2 by riešila **IKT riziká** vo finančnom sektore zlepšením schopností finančných inštitúcií čeliť incidentom IKT. To by viedlo k zníženiu rizika rýchleho šírenia kybernetických incidentov naprieč finančnými trhmi. Hoci je náročné odhadnúť náklady na prevádzkové incidenty vo finančnom sektore (nie všetky incidenty sú nahlasované, rozsah nákladov je neistý), odvetvové posúdenia naznačujú, že náklady finančného sektora EÚ by sa mohli pohybovať medzi 2 až 27 mld. EUR ročne. Uprednostňovanou možnosťou by sa zmiernili tieto priame náklady a všetky širšie vplyvy významných kybernetických incidentov na finančnú stabilitu. Odstránením prekrývajúcich sa **požiadaviek na nahlasovanie** by sa znížila administratívna záťaž. Napríklad niektoré z najväčších bánk by v tejto súvislosti mohli dosiahnuť úspory od 40 do 100 miliónov EUR ročne. Priame

podávanie hlásení by zároveň viedlo k zlepšeniu vedomostí orgánov dohľadu o incidentoch IKT. **Harmonizované testovacie** postupy by zvýšili mieru odhaľovania neznámych zraniteľností a rizík. Zároveň by sa nimi znížili náklady, najmä náklady cezhraničných spoločností. Napríklad celkové očakávané výhody spoločného prístupu k testovaniu by pre 44 najväčších cezhraničných bánk mohli dosiahnuť sumu 11 až 88 miliónov EUR. Zavedením koherentného súboru pravidiel riadenia rizík **externých poskytovateľov IKT služieb,** by finančné spoločnosti získali väčšiu kontrolu nad tým, ako externí poskytovatelia dodržiavajú regulačný rámec, čo by mohlo potešiť orgány dohľadu. Dohľad nad externými poskytovateľmi IKT by mal aj prudenciálne výhody. Celkovo sa uprednostňovaná možnosť premieta do širších spoločenských výhod, ktoré vyplývajú z odolnejšieho prevádzkového prostredia pre všetkých účastníkov finančných trhov, a posilnenej ochrany spotrebiteľov a investorov.

Aké sú náklady na uprednostňovanú možnosť (prípadne na hlavné možnosti, ak žiadna možnosť nemá prednosť)?

Uprednostňovaná možnosť by viedla k vzniku jednorazových aj opakovaných nákladov. Jednorazové náklady sú spôsobené investíciami do IT systémov a je ťažké vyčísliť ich vzhľadom na rozdielny stav pôvodných systémov spoločností. Keďže sa nevykonal regulačný zásah, niektoré finančné spoločnosti už investovali značné prostriedky do IKT systémov. Znamená to, že náklady veľkých finančných spoločností, ktoré budú vykonávať opatrenia podľa tohto návrhu, budú pravdepodobne nízke. Očakáva sa, že aj náklady menších spoločností budú nižšie, pretože tieto spoločnosti by podliehali menej prísnym opatreniam úmerným ich nižšiemu riziku. Pokiaľ ide o testovanie, európske orgány dohľadu odhadli, že náklady spojené s penetračným testovaním na základe konkrétnej hrozby sa pohybujú od 0,1 % do 0,3 % z celkového rozpočtu príslušných spoločností na IKT. Náklady spojené s nahlasovaním incidentov by sa výrazne znížili vďaka tomu, že tieto hlásenia by sa neprekrývali so správami podávanými v súvislosti so smernicou NIS. Orgánom dohľadu by v súvislosti s ich novými úlohami takisto vznikli určité náklady. Napríklad v prípade orgánov dohľadu, ktoré by sa zúčastňovali na priamom dohľade nad externými poskytovateľmi IKT, by sa mohlo očakávať zvýšenie ekvivalentu plného pracovného času o 1 až 5 ekvivalentov plného pracovného času v prípade vedúceho orgánu a o približne 0,25 ekvivalentu plného pracovného času v prípade zúčastnených orgánov.

Aký to bude mať vplyv na podniky, MSP a mikropodniky?

Uprednostňovaná možnosť by sa vzťahovala na všetky finančné spoločnosti, aby sa zvýšila prevádzková odolnosť daného sektora ako celku. Tento široký rozsah pôsobnosti je dôležitý vzhľadom na prepojenosť finančného sektora a s tým súvisiacu potrebu zaistiť všeobecne dobrú úroveň celkovej prevádzkovej odolnosti. Pri definovaní základných požiadaviek v hlavných oblastiach intervencie by sa však uplatňovala zásada proporcionality medzi subsektormi a aj v rámci každého subsektora. Okrem iného by sa zohľadňovali rozdiely v obchodných modeloch, veľkosti, rizikovom profile, systémovej významnosti atď. Napríklad opatrenia týkajúce sa nahlasovania incidentov a testovania by boli menej prísne pre menšie finančné spoločnosti.

Očakáva sa významný vplyv na štátne rozpočty a verejnú správu?

Nie. Ako už bolo vysvetlené, dodatočný dohľad si môže v obmedzenej miere vyžadovať dodatočné zdroje na dohľad, ktoré môžu byť celkovo alebo čiastočne (pokiaľ ide o poplatky za dohľad) kryté z verejných rozpočtov.

Očakávajú sa iné významné vplyvy?

Sociálno-ekonomické dôsledky pandémie ochorenia COVID-19 svedčia o kritickej povahe digitálnych finančných trhov a ich prevádzkovej odolnosti. Uprednostňovaná možnosť by vytvorila pevný základ pre využívanie digitálnej transformácie zaistením toho, že jednotný trh s finančnými službami vrátane bankovej únie a únie kapitálových trhov by boli prevádzkovo odolné na základe spoločného súboru pravidiel a požiadaviek, ktorých cieľom je bezpečnosť, výkonnosť, stabilita a rovnaké podmienky. To posilní aj pozíciu Európy ako svetového lídra v oblasti financií a digitálnych technológií, čo je cieľ, ktorý Komisia stanovila vo svojom oznámení Formovanie digitálnej budúcnosti Európy.

D. Ďalší postup

Kedy sa táto politika preskúma?

Prvé preskúmanie by sa uskutočnilo po troch rokoch od nadobudnutia účinnosti právneho nástroja. Komisia by poskytla správu o preskúmaní Európskemu parlamentu a Rade. Toto preskúmanie by mohlo byť podporené verejnou konzultáciou, štúdiami, odbornými diskusiami, prieskumami a prípadne seminármi.