Az Európai Unió
Tanácsa

Brüsszel, 2020. szeptember 24.
(OR. en)

Intézményközi referenciaszám:
2020/0268(COD)

11052/20
ADD 2

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

FEDŐLAP

Küldi:	az Európai Bizottság főtitkára részéről Jordi AYET PUIGARNAU igazgató
Az átvétel dátuma:	2020. szeptember 24.
Címzett:	Jeppe TRANHOLM-MIKKELSEN, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	SWD(2020) 204 final
Tárgy:	BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM A HATÁSVIZSGÁLATI JELENTÉS VEZETŐI ÖSSZEFOGLALÓJA amely a következő dokumentumot kíséri AZ EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE a 2006/43/EK irányelv, a 2009/65/EK irányelv, a 2009/138/EK irányelv, a 2011/61/EU irányelv, a 2013/36/EU irányelv, a 2014/65/EU irányelv, az (EU) 2015/2366 irányelv és az (EU) 2016/2341 irányelv módosításáról

Mellékelten továbbítjuk a delegációknak a SWD(2020) 204 final számú dokumentumot.

Melléklet: SWD(2020) 204 final

EURÓPAI
BIZOTTSÁG

Brüsszel, 2020.9.24.
SWD(2020) 204 final

This document corrects document SWD(2020) 204 final of 24.09.2020
Two references in the title of the cover page have been corrected.
Concerns the EN version only.
The text shall read as follows:

BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM

A HATÁSVIZSGÁLATI JELENTÉS VEZETŐI ÖSSZEFOGLALÓJA

amely a következő dokumentumot kíséri

AZ EURÓPAI PARLAMENT ÉS A TANÁCS IRÁNYELVE

a 2006/43/EK irányelv, a 2009/65/EK irányelv, a 2009/138/EK irányelv, a 2011/61/EU irányelv, a 2013/36/EU irányelv, a 2014/65/EU irányelv, az (EU) 2015/2366 irányelv és az (EU) 2016/2341 irányelv módosításáról

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

Vezetői összefoglaló

Hatásvizsgálat a pénzügyi ágazatbeli digitális működési rezilienciáról szóló rendeletre irányuló javaslatról

A. A fellépés szükségessége

Miért van szükség fellépésre? Milyen problémát kell megoldani?

A pénzügyi ágazat nagymértékben támaszkodik az információs és kommunikációs technológiákra (IKT). A jelenlegi Covid19-világjárvány valószínűleg felgyorsítja ezt, tekintettel a pénzügyi szolgáltatásokhoz való folyamatos távoli hozzáférés biztosításából adódó előnyökre. A digitális technológiák alkalmazása azonban aggályokat is felvet; a vállalkozásoknak képesnek kell lenniük arra, hogy esetleges IKT-zavarok esetén működőképesek maradjanak és szolgáltatásaikat fenntartva kezelni tudják a digitális biztonsági eseményeket és fenyegetéseket. Egy nagymértékben összekapcsolt pénzügyi ágazatban, amely a reálgazdaság számára alapvető fontosságú, határokon átnyúló szolgáltatásokat épít ki, az IKT-függőségből eredő sebezhetőségek – noha minden gazdasági ágazatban jelen vannak – különösen hangsúlyosak 1. az IKT mély és széles körű használata miatt, valamint 2. annak lehetősége miatt, hogy egy pénzügyi vállalkozásnál vagy egy pénzügyi alszektorban bekövetkező működési esemény hatásai gyorsan átterjednek más vállalkozásokra vagy a pénzügyi ágazat más részeire, és végső soron a gazdaság többi részére.

Annak ellenére, hogy a pénzügyi szektor a piaci és szabályozási integráció tekintetében igen fejlett, növekedését pedig egységes, harmonizált szabályrendszer – az uniós egységes szabálykönyv – segíti, a működési reziliencia iránti megnövekedett igényekre adott horizontális vagy ágazati szintű uniós válasz vagy:

- minimális harmonizáción alapult, teret hagyva a nemzeti értelmezésnek és az egységes piacon belüli széttagolódásnak, vagy
- túl általános és korlátozottan alkalmazható volt, változó mértékben kezelve az általános működési kockázatot, részlegesen szabályozva a digitális működési *reziliencia* egyes elemeit (például az IKT-kockázatkezelést, az események bejelentését és a harmadik felek IKT-kockázatát), másokat ugyanakkor kihagyva (tesztelés).

Az uniós beavatkozás eddig nem kezelte a működési kockázatot oly módon, ami megfelelne a pénzügyi vállalkozások azon igényeinek, hogy ellenálljanak az IKT-val kapcsolatos sebezhetőségeknek, elhárítsák ezeket, majd helyreállítsák működésüket, továbbá nem biztosítja a pénzügyi felügyeletek számára sem az ahhoz szükséges eszközöket, hogy eleget tegyenek az IKT sebezhetőségéből eredő pénzügyi instabilitás megfékezésére vonatkozó megbízatásuknak.

A jelenlegi hiányosságok és következetlenségek a nem koordinált nemzeti kezdeményezések (például a teszteléssel kapcsolatosak) és felügyeleti megközelítések (például az IKT harmadik felektől való függőségével kapcsolatosak) elterjedéséhez vezettek, ami vagy átfedéseket, a követelmények megkettőzését és határokon átnyúlóan tevékenykedő pénzügyi vállalkozások számára magas adminisztratív és megfelelési költségeket eredményez, vagy azt, hogy az IKT-kockázatokat nem tárják fel és nem kezelik. Összességében nem biztosított a pénzügyi ágazat stabilitása és integritása, a pénzügyi szolgáltatások egységes piaca pedig továbbra is széttöredezett, aminek következtében a gyengül a fogyasztó- és befektetővédelem.

Mi a kezdeményezés várható eredménye?

Az általános célkitűzés az uniós pénzügyi ágazat digitális működési rezilienciájának megerősítése a meglévő uniós pénzügyi jogszabályok észszerűsítése és továbbfejlesztése, valamint új követelmények bevezetése révén ott, ahol hiányosságok vannak, azzal a céllal, hogy:

- javuljon a pénzügyi vállalkozásoknál az IKT-kockázatok kezelése;
- bővüljenek a felügyeletek fenyegetésekkel és biztonsági eseményekkel kapcsolatos ismeretei;
- javuljon a pénzügyi vállalkozásoknál az IKT-rendszerek tesztelése; valamint
- jobb legyen az abból eredő kockázatok felügyelete, hogy a pénzügyi vállalkozások harmadik fél IKT-szolgáltatóktól függenek.

Konkrétabban, a javaslat koherensebb és következetesebb mechanizmusokat hozna létre az események jelentésére, ezáltal csökkentené a pénzügyi intézmények adminisztratív terheit és megerősítené a felügyeleti hatékonyságot.

Milyen többletértéket képvisel az uniós szintű fellépés?

A pénzügyi szolgáltatások európai egységes piacára uniós szinten meghatározott, kiterjedt szabályrendszer vonatkozik, amely európai útlevél révén lehetővé teszi a tagállamok valamelyikében engedélyezett pénzügyi vállalkozások számára, hogy a teljes egységes piacon szolgáltatásokat nyújtsanak. Ebből adódóan nemzeti szintű szabályokkal nem erősíthető eredményesen a pénzügyi vállalkozások digitális működési rezilienciája. Emellett – a pénzügyi válság nyomán – az egységes uniós szabálykönyv igen részletes előírásokat tartalmaz az olyan „hagyományosabb” kockázatokra vonatkozóan, mint a hitelezési, a piaci, a partner- és a likviditási kockázat. A működési kockázatra vonatkozó rendelkezések továbbra is általános jellegűek. A digitális működési

reziliencia megerősítése a működési kockázatra vonatkozóan jelenleg is uniós szinten meghatározott rendelkezések módosítását igényli, amelyek ennélfogva ugyancsak uniós szinten korszerűsíthetők és egészíthetők ki.

B. Megoldások

Milyen jogalkotási és nem jogalkotási szakpolitikai alternatívák merültek fel? Van-e előnyben részesített megoldás? Miért?

A hatásvizsgálat az intézkedés nélküli alapforgatókönyv mellett három alternatívát mérlegelt a pénzügyi szolgáltatásokra vonatkozó uniós jogszabályok kapcsán. Konkrétabban:

- **Nincs intézkedés**: a digitális működési reziliencia szabályait továbbra is a pénzügyi szolgáltatásokra vonatkozó jelenlegi, sokrétű uniós rendelkezések: részben a kiberbiztonsági irányelv, részben pedig a meglévő vagy jövőbeli nemzeti rendszerek határoznák meg;
- **1. alternatíva – a tőkepufferek megerősítése**: további tőkepuffer bevezetése, amely növeli a pénzügyi vállalkozások veszteségviselő képességét a digitális működési reziliencia hiányával összefüggésben;
- **2. alternatíva – a pénzügyi szolgáltatások digitális működési rezilienciájára vonatkozó jogi aktus**: átfogó uniós szintű keret bevezetése, amely minden szabályozott pénzügyi intézmény számára meghatározza a digitális működési reziliencia szabályait, és ezáltal:
  - átfogóbb jelleggel kezeli az IKT-kockázatokat;
  - hozzáférhetővé teszi a pénzügyi felügyeletek számára az IKT-vonatkozású biztonsági eseményekkel kapcsolatos információkat;
  - biztosítja, hogy a pénzügyi vállalkozások értékeljék a megelőző és a rezilienciára irányuló intézkedéseiket, és azonosítsák az IKT-sebezhetőségeket;
  - megerősíti a harmadik félnek minősülő IKT-szolgáltatók közvetett felvigyázására vonatkozó kiszervezési szabályokat;
  - lehetővé teszi a harmadik félnek minősülő IKT-szolgáltatók tevékenységének közvetlen felvigyázását, amikor pénzügyi vállalkozásoknak nyújtanak szolgáltatásokat;
  - ösztönzi a fenyegetettséggel kapcsolatos információk cseréjét a pénzügyi ágazaton belül.
- **3. alternatíva – a rezilienciára vonatkozó jogi aktus a harmadik félnek minősülő kulcsfontosságú szolgáltatók központosított felügyeletével ötvözve**: a digitális működési rezilienciára vonatkozó jogi aktus mellett új hatóság létrehozása az olyan harmadik félnek minősülő IKT-szolgáltatók felügyelete céljából, amelyek pénzügyi vállalkozásoknak nyújtanak kritikus IKT-szolgáltatásokat. Az alternatíva ezenkívül egyértelműbben körülhatárolná a kiberbiztonsági irányelv alkalmazási körét a pénzügyi ágazattal összefüggésben.

Az előnyben részesített megoldás a 2. alternatíva. A többi alternatívához képest ez valósítja meg a kezdeményezés legtöbb célkitűzését, ugyanakkor figyelembe veszi a hatékonyság és a koherencia kritériumait is. Az érdekelt felek is leginkább ezt az alternatívát támogatják.

Ki melyik alternatívát támogatja?

Az érdekelt felek többsége (a magán- és a közszektorban egyaránt) egyetért abban, hogy a pénzügyi vállalkozások digitális működési rezilienciájának jobb védelméhez uniós fellépésre van szükség. Emellett sokuk szerint van szükség uniós fellépésre az abból eredő szabályozási terheknek a csökkentéséhez is, hogy a pénzügyi vállalkozások a kiberbiztonsági irányelvben, a pénzügyi szolgáltatásokra vonatkozó uniós jogszabályokban, valamint a nemzeti rendszerekben rögzített párhuzamos vagy egymásnak ellentmondó szabályok hatálya alá tartoznak (például a biztonsági események bejelentése tekintetében). Ennek megfelelően az érdekelt felek közül kevesen támogatják azt, hogy ne legyen intézkedés. Kevesen tartják célszerűnek továbbá a digitális működési reziliencia megnövelt tőkepufferek (1. alternatíva) útján történő védelmét is. Mivel ugyanakkor ez a működési kockázat kezelésének hagyományos megközelítése, különösen a bankszektorban, ennek megfelelően pl. a nemzetközi szabványügyi testületek figyelembe veszik. A nyilvános konzultációban részt vevő érdekelt felek széles köre támogatja az olyan kvalitatív intézkedéseket, amelyek a 2. alternatíva szerint észszerűsítenék és korszerűsítenék az uniós pénzügyi jogszabályokat, hiányosság esetén új követelményeket vezetnének be, mindeközben pedig megtartanák a kapcsolódási pontokat a horizontális kiberbiztonsági irányelvvel, . Míg egyes (főként közszektorbeli) érdekelt felek célszerűnek tartják a harmadik félnek minősülő IKT-szolgáltatók 3. alternatíva szerinti megerősített felügyeletét, kisebb a támogatottsága egy új uniós hatóság e célból történő létrehozásának és a kiberbiztonsági keretről való nagyobb mértékű leválasztásnak.

C. Az előnyben részesített alternatíva hatásai

Melyek az előnyben részesített alternatíva (ha nincs ilyen, akkor a főbb lehetőségek) előnyei?

A 2. alternatíva a teljes pénzügyi ágazatban azáltal kezelné az **IKT-kockázatokat**, hogy javítja a pénzügyi

intézmények képességét az IKT-vonatkozású biztonsági események elviselésére. Ez csökkentené egy kiberbiztonsági esemény pénzügyi piacokon keresztüli gyors terjedésének kockázatát. Noha a pénzügyi ágazatban előforduló váratlan működési események költsége nehezen becsülhető (nem minden eseményt jelentenek be; a költségek terjedelme bizonytalan), az ágazati felmérések alapján az uniós pénzügyi ágazatot évente 2–27 milliárd EUR összegű költség terhelheti. Az előnyben részesített alternatíva mérsékelné ezeket a közvetlen költségeket, valamint a jelentősebb kiberbiztonsági események pénzügyi stabilitásra gyakorolt általánosabb hatásait is. A **bejelentési követelmények** átfedéseinek megszüntetése csökkentené az adminisztratív terheket. Ezzel összefüggésben például a legnagyobb bankok közül egyesek 40–100 millió EUR közötti költséget takaríthatnak meg. A közvetlen bejelentés révén a felügyeletek több információt kapnának az IKT-vonatkozású biztonsági eseményekről is. A **tesztelési módszerek harmonizálása** növelné az ismeretlen sebezhetőségek és kockázatok felderítési arányát. Emellett csökkentené költségeket is, különösen a határokon átnyúló tevékenységű vállalkozások számára. Például a 44 legnagyobb határokon átnyúló tevékenységű bank számára a közös tesztelési módszer várható gazdasági előnye 11–88 millió EUR közé tehető. A **harmadik félnek minősülő IKT-szolgáltatókkal** kapcsolatos kockázatok kezelésére vonatkozó koherens szabályok bevezetésével a pénzügyi vállalkozások jobban ellenőrizhetnék a harmadik félnek minősülő szolgáltatók szabályozási keretnek való megfelelését, ami felügyeleti szempontból is megnyugtató lehet. Emellett a harmadik félnek minősülő IKT-szolgáltatók felügyeleti felvigyázásából prudenciális előnyök is származnának. Összességében az előnyben részesített alternatíva szélesebb körű társadalmi előnyökkel jár egyrészt a fogyasztók és a befektetők megerősített védelme, másrészt amiatt, hogy valamennyi pénzügyi piaci szereplő működési környezete reziliensebbé válik.

Milyen költségekkel jár az előnyben részesített alternatíva (ha nincs ilyen, akkor milyen költségekkel járnak a főbb lehetőségek)?

Az előnyben részesített alternatívával összefüggésben egyszeri és ismétlődő költségek is felmerülnének. Az előbbiek az informatikai rendszerekre irányuló beruházásokból adódnak, és a vállalkozások hagyományos rendszereinek eltérő állapota miatt nehezen számszerűsíthetők. Szabályozói beavatkozás hiányában egyes pénzügyi vállalkozások eddig is jelentős beruházásokat hajtottak végre IKT-rendszereik terén. Ez azt jelenti, hogy a pénzügyi nagyvállalatokat illetően az e javaslatban foglalt intézkedések végrehajtása valószínűleg csekély hatású lesz. A költségek várhatóan alacsonyabbak lesznek a kisebb vállalkozások esetében is, amelyekre mérsékeltebb kockázatukkal arányosan kevésbé szigorú intézkedések vonatkoznának. A tesztelést illetően az európai felügyeleti hatóságok becslése szerint a fenyegetettségi szempontú behatolási tesztelés költségei az érintett vállalkozások IKT-költségvetésének 0,1–0,3 %-ára tehetők. A biztonsági események bejelentésével kapcsolatos költségek drasztikusan visszaesnének, mivel a kiberbiztonsági adatszolgáltatásban nem lennének átfedések. Bizonyos költségek a felügyeleteknél is felmerülnének a többletfeladatokból adódóan. Például a harmadik félnek minősülő IKT-szolgáltatók közvetlen felvigyázásában részt vevő felügyeleteknél a teljes munkaidős egyenértékben kifejezett létszámnövekedés várhatóan a vezető hatóság esetében 1–5 fő, a további részt vevő hatóságok esetében mintegy 0,25 fő.

Hogyan érinti a fellépés a vállalkozásokat, köztük a kis- és középvállalkozásokat és a mikrovállalkozásokat?

Az előnyben részesített alternatíva alkalmazási köre valamennyi pénzügyi vállalkozásra kiterjedne annak érdekében, hogy a teljes ágazat digitális működési rezilienciája fokozódjon. A széles alkalmazási kör fontos a pénzügyi ágazat összekapcsolt jellegére és arra az ebből adódó igényre tekintettel, hogy a teljes ágazat digitális működési rezilienciája elfogadható mértékű legyen. A fő beavatkozási területeket átfogó alapvető követelmények meghatározásakor ugyanakkor az arányosság elve az alágazatokban együttesen és az egyes alágazatokon belül is érvényesülne. A fellépés figyelembe venné többek között az üzleti modellek, a méret, a kockázati profil, a rendszerszempontú jelentőség stb. eltéréseit. Például a kisebb vállalkozások esetében a biztonsági események bejelentésére és a tesztelésre vonatkozó intézkedések kevésbé lennének szigorúak.

Jelentős lesz-e a tagállamok költségvetésére és közigazgatására gyakorolt hatás?

Az előzőekben kifejtett módon a felvigyázási többletfeladatok miatt a felügyeleteknek csak kismértékben szükséges bővíteniük az erőforrásaikat, amelynek költsége teljes egészében, illetve a felügyeleti díjak esetében részben az állami költségvetésekből finanszírozható.

Lesznek-e egyéb jelentős hatások?

A Covid19-világjárvány társadalmi-gazdasági következményei jelzik a digitális pénzügyi piacok és működési rezilienciájuk kritikus jelentőségét. Az előnyben részesített alternatíva stabil alapokat teremtene a digitális transzformáció kiaknázásához azzal, hogy a biztonságra, a teljesítményre, a stabilitásra és az egyenlő versenyfeltételekre irányuló közös szabály- és követelményrendszer révén biztosítja a digitális működési rezilienciát a pénzügyi szolgáltatások egységes uniós piacán, beleértve a bank- és a tőkepiaci uniót is. Mindez

egyúttal erősíti Európa pénzügyi és digitális vezető pozícióját a világon, amelyet a Bizottság célkitűzésként fogalmazott meg az „Európa digitális jövőjének megtervezése” című közleményében.

D. További lépések

Mikor kerül sor a szakpolitikai fellépés felülvizsgálatára?

Az első felülvizsgálatra három évvel a jogi eszköz hatálybalépését követően kerülne sor. A Bizottság jelentést nyújtana be a felülvizsgálatról az Európai Parlamentnek és a Tanácsnak. A felülvizsgálat adott esetben nyilvános konzultációra, tanulmányokra, szakértői megbeszélésekre, felmérésekre és munkaértekezletekre támaszkodhat.