EUROOPA
KOMISJON

Brüssel, 24.9.2020
SWD(2020) 199 final

KOMISJONI TALITUSTE TÖÖDOKUMENT

MÕJU HINDAMISE ARUANDE KOMMENTEERITUD KOKKUVÕTE

Lisatud dokumendile:

Ettepanek: Euroopa Parlamendi ja nõukogu määrus,

mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014 ja (EL) nr 909/2014

{COM(2020) 595 final} - {SEC(2020) 307 final} - {SWD(2020) 198 final}

Kommenteeritud kokkuvõte

Mõjuhinnang järgmise ettepaneku kohta: määrus, mis käsitleb finantssektori digitaalset tegevuskerksust

A. Vajadus meetmete järele

Miks? Mis on lahendamist vajav probleem?

Finantssektor sõltub suurel määral info- ja kommunikatsioonitehnoloogiast (IKT). Praegune COVID-19 pandeemia tõenäoliselt suurendab seda sõltuvust, pidades silmas kasu, mis tuleneb finantsteenustele pideva kaugjuurdepääsu tagamisest. Digitehnoloogiast sõltuvusega kaasnevad aga ka probleemid. Ettevõtjad peavad suutma võimalike IKT-katkestustega toime tulla, et digiintsidente ja -ohte saaks käsitleda ja teenuseid säilitada. Finantssektoris, kus on väga tihedad sidemed ja osutatakse elutähtsaid piiriüleseid teenuseid, millest sõltub reaalmajandus, on IKTst sõltumisest tingitud haavatavus (mis esinevad tegelikult kõigis majandussektorites) eriti suur, sest 1) IKTd kasutatakse sügavalt ja laialdaselt ning 2) ühes finantssektori ettevõtjas või finantssektori allsektoris toimunud tegevusintsidendi mõju võib kanduda kiiresti teistesse ettevõtjatesse või finantssektori teistesse osadesse ning lõpuks ülejäänud majandusse.

Kuigi finantssektoris on turgude ja õiguslik integratsioon väga kaugele jõudnud ning seal kasutatakse edukalt ühtlustatud õigusnorme – ELi ühtset reeglistikku –, on ELi reaktsioon suurematele tegevuskerksuse vajadustele nii horisontaalsel kui ka valdkondlikul tasandil kas

- põhinenud minimaalsel ühtlustamisel, jättes niiviisi ruumi riiklikule tõlgendamisele ja ühtse turu killustumisele, või
- olnud liiga üldine ja piiratud ulatusega, käsitledes üldist operatsiooniriski erinevas mahus, reguleerides osaliselt digitaalse tegevus*kerksuse* mõningaid komponente (nt IKT-riskide juhtimine, intsidentidest teatamine ja kolmandast isikust tulenev IKT-risk) ja jättes teised (testimine) kõrvale.

EL ei ole oma sekkumise raames seni käsitlenud operatsiooniriski viisil, mis vastaks finantssektori ettevõtjate vajadusele tulla IKTga seotud haavatavustega toime, reageerida neile ja neist taastuda, samuti ei ole antud finantsjärelevalveasutustele vahendeid, et nad saaksid täita ülesannet piirata IKTga seotud haavatavustest tulenevat finantsilist ebastabiilsust.

Praegused lüngad ja ebaühtlus on toonud kaasa koordineerimata riiklikud algatused (nt testimise kohta) ja järelevalvealased lähenemisviisid (mis käsitlevad näiteks sõltuvust IKT-teenuseid osutavatest kolmandatest isikutest), mis väljenduvad kas kattuvuses, nõuete dubleerimises ja suurtes haldus- ja nõuete täitmise kuludes piiriüleste finantssektori ettevõtjate jaoks või IKT-riskide avastamata ja käsitlemata jäämises. Kokkuvõttes ei ole finantssektori stabiilsus ja usaldusväärsus tagatud ning finantsteenuste ühtne turg on killustunud, mille tagajärjeks on tarbijate ja investorite nõrgem kaitse.

Mida selle algatusega loodetakse saavutada?

Üldeesmärk on tugevdada ELi finantssektori digitaalset tegevuskerksust ning ühtlustada ja ajakohastada kehtivaid finantsalaseid ELi õigusakte ning kehtestada lünkade korral uusi nõudeid, mille eesmärk on

- parandada finantssektori ettevõtjates IKT-riskide juhtimist;
- suurendada järelevalveasutuste teadmisi ohtudest ja intsidentidest;
- parandada finantssektori ettevõtjates IKT-süsteemide testimist ja
- jälgida paremini riske, mis tulenevad finantssektori ettevõtjate sõltuvusest kolmandast isikust IKT-teenuste osutajatest.

Ettepanekuga loodaks sidusamad ja ühtsemad intsidentidest teatamise mehhanismid ning vähendataks seega finantsasutuste halduskoormust ja suurendataks järelevalve tõhusust.

Milline on ELi tasandi meetmete lisaväärtus?

ELi finantsteenuste ühtset turgu reguleerivad rohked ELi tasandil sätestatud normid, mis tänu ELi tegevusloale võimaldavad ühes liikmesriigis loa saanud finantssektori ettevõtjatel osutada teenuseid kogu ühtsel turul. Sellest tulenevalt ei oleks riikliku tasandi normid tulemuslik viis ELi tegevusluba kasutavate finantssektori ettevõtjate tegevuskerksuse tugevdamiseks. Lisaks sisaldab ELi ühtne reeglistik finantskriisi tõttu väga üksikasjalikke ja ettekirjutavaid norme, mis käsitlevad rohkem traditsioonilisi riske, nagu krediidi-, turu-, vastaspoole ja likviidsusrisk. Kehtivad sätted operatsiooniriski kohta on üldised. Digitaalse tegevuskerksuse tugevdamiseks tuleb kohandada operatsiooniriske käsitlevaid sätteid, mis on ELi tasandil juba sätestatud ning mida saab seega ajakohastada ja täiendada ainult ELi tasandil.

B. Lahendused

Milliseid seadusandlikke ja mitteseadusandlikke poliitikavariante on kaalutud? Kas on olemas eelistatud variant? Miks?

Mõjuhinnangus kaaluti baasstsenaariumi, mille kohaselt ei võeta ELi finantsteenuste õigusaktidega seoses mingeid meetmeid, ja kolme muud varianti. Täpsemalt:

- **„ei tee midagi“** – tegevuskerksuse norme kehtestataks jätkuvalt olemasolevate, lahknevate sätetega ELi finantsteenuste kohta, osaliselt küberturvalisuse direktiiviga ja kehtivate või tulevaste riiklike kordadega;
- **variant 1 – suuremad kapitalipuhvrid**: kehtestataks täiendav kapitalipuhver, et suurendada finantssektori ettevõtjate võimet katta kahjum, mis võib tuleneda tegevuskerksuse puudumisest;
- **variant 2 – finantsteenuste digitaalset tegevuskerksust käsitlev õigusakt**: ELi tasandil kehtestataks laiahaardeline raamistik, millega sätestataks kõiki reguleeritud finantsasutusi puudutavad digitaalse tegevuskerksus normid, mis
    - käsitlevad IKT-riske põhjalikumalt,
    - võimaldavad finantsjärelevalveasutustel pääseda juurde teabele IKTga seotud intsidentide kohta,
    - tagavad, et finantssektori ettevõtjad hindavad oma ennetus- ja kerksusmeetmete tulemuslikkust ning teevad kindlaks IKTga seotud haavatavused;
    - karmistavad tegevuse edasiandmise norme, mis reguleerivad kaudset järelevalvet kolmandast isikust IKT-teenuste osutajate üle;
    - võimaldavad teha otsest järelevalvet kolmandast isikust IKT-teenuste osutajate tegevuse üle, kui nad osutavad teenuseid finantssektori ettevõtjatele, ja
    - lisaks soodustavad ohuteadmuse vahetamist finantssektoris;
- **variant 3 – tegevuskerksust käsitlev õigusakt koos tsentraliseeritud järelevalvega kriitilise tähtsusega kolmandast isikust teenuseosutajate üle**: lisaks finantsteenuste digitaalset tegevuskerksust käsitleva õigusakti kehtestamisele (variant 2) loodaks uus asutus, mis teeks järelevalvet kolmandast isikust IKT-teenuste osutajate üle, mis osutavad finantssektori ettevõtjatele kriitilise tähtsusega IKT-teenuseid. Selle variandiga eraldataks finantssektor selgemalt küberturvalisuse direktiivi kohaldamisalast.

Variant 2 on eelistatud variant. Võrreldes teiste variantidega saavutataks sellega enamik algatuse eesmärke, võttes samal ajal arvesse tõhususe ja ühtsuse kriteeriume. Seda varianti toetavad kõige enam ka sidusrühmad.

Kes millist varianti toetab?

Enamik sidusrühmi (era ja avalik sektor) nõustub, et finantssektori ettevõtjate tegevuskerksuse paremaks kaitsmiseks on vaja ELi meedet. Paljud usuvad, et ELi meede on vajalik ka selleks, et vähendada regulatiivset koormust, mida tekitavad finantssektori ettevõtjatele nende suhtes kohaldatavad dubleerivad ja ebajärjekindlad normid, mis on sätestatud küberturvalisuse direktiivis, ELi finantsteenuseid käsitlevas õiguses ja riiklikes kordades (nt intsidentidest teatamise puhul). Ainult mõni sidusrühm on seisukohal, et ei peaks tegema midagi. Mõni üksik sidusrühm leiab, et tegevuskerksust tuleks kaitsta suuremate kapitalipuhvrite abil (variant 1). See on aga traditsiooniline lähenemine operatsioonriskile, eelkõige panganduses, ning seda kaaluvad näiteks rahvusvaheliste standardite kehtestajad. Avalikus konsultatsioonis osalenud sidusrühmad toetavad laialdaselt variandis 2 kirjeldatud kvalitatiivseid meetmeid, mis ühtlustaksid ja ajakohastaksid ELi finantsalaseid õigusakte ning millega kehtestataks lünkade korral uued nõuded, säilitades samal ajal seosed horisontaalse küberturvalisuse direktiiviga. Kuigi mõned sidusrühmad (eelkõige avalik sektor) näevad kasu, mida annaks tugevam järelevalve kolmandast isikust IKT-teenuste osutajate üle (variant 3), leidsid sel eesmärgil uue ELi asutuse loomine ja selgem kaugenemine võrgu- ja infosüsteemide turvalisuse raamistikust sidusrühmade hulgas ainult vähest toetust.

C. Eelistatud poliitikavariandi mõju

Millised on eelistatud poliitikavariandi (kui see on olemas, vastasel korral peamiste poliitikavariantide) eelised?

Variandi 2 puhul käsitletaks kogu finantssektori **IKT-riske**, suurendades finantsasutuste suutlikkust tulla IKT-intsidentidega toime. See vähendaks riski, et küberintsident hakkab finantsturgudel kiiresti levima. Kuigi tegevusintsidentide kulusid on finantssektoris keeruline hinnata (kõigist intsidentidest ei teatata, kulude maht ei ole kindel), lubavad sektori hinnangud arvata, et ELi finantssektori kulud võivad olla 2–27 miljardit eurot aastas. Eelistatud variant vähendaks neid otseseid kulusid ja laiemat mõju, mida olulised küberintsidendid võivad finantsstabiilsusele avaldada. Kui kaotataks kattuvad **aruandlusnõuded**, väheneks halduskoormus. Näiteks võib mõningate suuremate pankade kokkuhoid sellisel juhul olla aastas 40–100 miljonit eurot. Otsene aruandlus suurendaks ka järelevalveasutuste teadmisi IKT-intsidentidest. **Ühtlustatud testimine** aitaks avastada rohkem haavatavusi ja riske. See vähendaks ka kulusid, eelkõige piiriüleste ettevõtjate jaoks. Kui testimisel kasutataks ühtset lähenemisviisi, võiks näiteks 44 suurima piiriülese panga kogu eeldatav kasu olla 11–88 miljonit eurot. Kui kehtestataks ühtsed normid **kolmandast isikust IKT-teenuste osutajate** riskide juhtimisele, oleks finantssektori ettevõtjatel rohkem kontrolli selle üle, kuidas kolmandast isikust teenuseosutajad õigusraamistikku järgivad, ning

see oleks abiks järelevalveasutustele. Järelevalve kolmandast isikust IKT-teenuste osutajate üle oleks kasulik ka usaldatavusnõuete puhul. Kokkuvõttes toob eelistatud variant laiemat ühiskondlikku kasu, mis tuleneb vastupidavamast tegevuskeskkonnast kõigi finantsturuosaliste jaoks ning tarbijate ja investorite tugevamast kaitsest.

Millised on eelistatud poliitikavariandi (kui see on olemas, vastasel korral peamiste poliitikavariantide) kulud?

Eelistatud variandiga kaasneksid nii ühekordsed kui ka korduvad kulud. Ühekordsed kulud tulenevad IT-süsteemidesse investeerimisest ja neid on keeruline kvantifitseerida, kuna ettevõtjate pärandsüsteemide seis on erinev. Kuna reguleerivat sekkumist ei ole olnud, on mõni finantssektori ettevõtja juba teinud IKT-süsteemidesse märkimisväärseid investeeringuid. See tähendab, et suurte finantssektori ettevõtjate jaoks on kõnealuse ettepaneku kohaste meetmete rakendamise kulud tõenäoliselt väikesed. Ka väiksemate ettevõtjate kulud on eeldatavasti väiksemad, sest nende suhtes kohaldataks leebemaid meetmeid, mis on proportsionaalsed nende väiksema riskiga. Mis puudutab testimist, siis Euroopa järelevalveasutuste hinnangu kohaselt moodustavad ohuteabel põhineva läbistustestimisega seotud kulud 0,1 %–0,3 % asjaomaste ettevõtjate IKT kogueelarvest. Intsidentidest teatamisega seotud kulud väheneksid järsult, sest ei oleks kattuvusi küberturvalisuse direktiivi kohase aruandlusega. Järelevalveasutustele tekiksid mõned kulud lisaülesannete tõttu. Näiteks kui vaadata kolmandast isikust IKT-teenuste osutajate üle tehtavas otseses järelevalves osalevate järelevalveasutuste täistööajale taandatud töötajate arvu, siis võib eeldada, et see suureneb juhtivas asutuses hinnanguliselt 1–5 töötaja võrra ja osalevates asutustes ligikaudu 0,25 töötaja võrra.

Milline on mõju ettevõtjatele, VKEdele ja mikroettevõtjatele?

Eelistatud variant hõlmaks kõiki finantssektori ettevõtjaid, et suurendada sektori kui terviku tegevuskerksust. Selline lai kohaldamisala on oluline, kuna finantssektoris on palju sidemeid ja seetõttu on vaja usaldusväärsel tasemel üldist tegevuskerksust. Sekkumise peamistes valdkondades põhinõuete kindlaksmääramisel kohaldataks proportsionaalsuse põhimõtet nii allsektorite lõikes kui ka iga allsektori sees. Arvesse võetaks muu hulgas ka ärimudelite, suuruse, riskiprofiili ja süsteemse olulisuse erinevusi. Näiteks oleksid intsidentidest teatamise ja testimise meetmed väiksemate finantssektori ettevõtjate puhul leebemad.

Kas on ette näha märkimisväärset mõju riigieelarvetele ja ametiasutustele?

Ei. Nagu mainitud eespool, võib täiendavaks järelevalveks olla vaja piiratud hulgal täiendavaid järelevalveressursse, mida võidakse täielikult või osaliselt (järelevalvetasude korral) rahastada avaliku sektori eelarvest.

Kas on oodata muud olulist mõju?

COVID-19 pandeemia sotsiaal-majanduslikud tagajärjed näitavad digitaalsete finantsturgude ja nende tegevuskerksuse kriitilist tähtsust. Eelistatud variant looks kindla aluse digiülemineku ärakasutamiseks, tagades, et finantsteenuste ühtne turg, sealhulgas pangandus- ja kapitaliturgude liidud, on tegevuskerksad ning lähtuvad ühistest normidest ja nõuetest, mille eesmärk on turvalisus, suutlikkus, stabiilsus ja võrdsed tingimused. Lisaks tugevdab see maailmas Euroopa positsiooni finants- ja digivaldkonna liidrina, mille komisjon seadis eesmärgiks oma teatises „Euroopa digituleviku kujundamine“.

D. Järelmeetmed

Millal poliitika läbi vaadatakse?

Esimene läbivaatamine tehtaks kolm aastat pärast õigusakti jõustumist. Komisjon esitaks Euroopa Parlamendile ja nõukogule läbivaatamise kohta aruande. Läbivaatamist toetaksid vastavalt vajadusele avalikud konsultatsioonid, uuringud, arutelud ekspertidega, küsitlused ja seminarid.