**Lisa 1. Arvamused digirahanduse paketi kohta**

| Nr | Sisu | Arvestatud/ mittearvestatud/ selgitatud |
|---|---|---|
| **1** | **Majandus- ja Kommunikatsiooniministeerium** | |
| | MKMi kommentaarid EL digirahanduse strateegia paketi osas. Üldiselt läheb digirahanduse ettepanek kokku ka sellega, millega Eesti Pank täna tegeleb ning strateegias välja toodud ideed tunduvad toetavad ka meie tugevamate fintech startupide tegevuste osas (Veriff, Salv jne). | |
| | Digirahanduse strateegia dokumendis punktis 4.3 välja toodud *andmepõhise innovatsiooni edendamine rahanduses ühise finantsandmeruumi loomise kaudu.* Lisaks on välja toodud järgmist: *„Kogu korraldatud finantsteabele reaalajas digitaalse juurdepääsu hõlbustamine 2024. aastaks tuleks ELi finantsteenuseid käsitlevate õigusaktide kohaselt avaldatav teave avalikustada standardses ja masinloetavas vormingus. Kapitaliturgude liidu tegevuskava raames arendab komisjon ELi taristut, et hõlbustada juurdepääsu kogu kapitaliturgudega seotud avalikule teabele.“* Ning lk 13 on välja toodud, et *„uuenduslike IT-vahendite edendamine aruandluse ja järelevalve hõlbustamiseks kavatseb EL luua 2024. aastaks vajalikud tingimused, mis võimaldavad kasutada uuenduslikke tehnoloogiad, sealhulgas regulatiiv- ja järelevalvetehnoloogia vahendeid reguleeritud üksuste järelevalvelise aruandluse ja ametiasutuste poolse järelevalve jaoks.“* Peame seda lähenemist oluliseks, Eesti juhib Läänemere strateegia suunal reaalaja majanduse projekti, mille eesmärk on reaalaja majanduse võimaluste kasutuselevõtt Põhjamaade ja Läänemereriikide poolt. Leiame, et komisjoni poolt kavandatav haakub meie tegevusega reaalaja majanduse edendamisel ning edastame võimalikud täiendavad kommentaarid 6. novembriks (saatsime ITLile palve tagasisideks ning ootame veel ka nende võimalikku tagasisidet). | |
| | Küberturvalisuse valdkonna osas toome välja, et kuivõrd 19.10 saatsime arvamuse operatsioonilise resilientsuse akti (DORA) kohta, kattuvad meie ettepanekud ning ka eelviidatud arvamuse osas põhimõtted püsivad. | |
| | **Majandus- ja Kommunikatsiooniministeeriumil on finantsteenuste digitaalse operatsioonilise resilientsuse akti (DORA) ettepaneku kohta järgmised märkused:** | |
| | On mõistetav, et nn IT-kriitilisemad sektorid nagu finantssektor seavad teenusepakkujatele karmimad küberturvalisuse nõuded. Võrgu- ja infosüsteemide turvalisuse direktiiv (NIS direktiiv) peaks seejuures jääma üldregulatsiooniks. DORA määruses olev küberturvalisuse tase peaks olema vähemalt NIS direktiivi tasemel (NIS direktiivi art 1(7)), kuid kuna NIS direktiiv on ülevaatusel ning selle sisu tõenäoliselt muutub, võib juhtuda, et tulevased NIS muudatused tekitavad vajadust ka DORA sisu muuta. Vastuolusid tulevase NIS direktiivi järglase ja DORA määruse vahel on mõistlik ennetada. | |
| | DORA ettepanekus kasutatavad küberturvalisuse mõisted ja nende sisu olulise mõjuga intsidendist teavitamisel peaks NIS direktiivi ja DORA vahel olema harmoneeritud. Dubleerimist ja eri õigusaktides küberturvalisuse põhimõistetele eri sisu andmist tuleks vältida (nt „tõsine“ küberintsident DORA ettepanekus ja „olulise mõjuga“ küberintsident NIS direktiivis). | |

| | | |
|---|---|---|
| | Küberintsidentidest teavitamisel võiks vähemalt suurematel teenusepakkujatel olla kohustus teavitada ka kriitilistest haavatavustest. Eesti valitsus on teinud Euroopa Komisjonile NIS direktiivi ülevaatuse avaliku konsultatsiooni raames ettepaneku hõlmata küberintsidendi mõistesse sündmus, mis ohustab süsteemi turvalisust.1 Eesti küberturvalisuse seaduses on küberintsident defineeritud kui süsteemis toimuv sündmus, mis ohustab või kahjustab süsteemi turvalisust. Nii NIS direktiivis kui ka DORA ettepanekus on praegu intsident defineeritud kitsamalt - sündmus, mis kahjustab süsteemi turvalisust. | |
| | Küberintsidentidest raporteerimisega seoses on peamine, et operatiivne info küberintsidendi kohta jõuaks koheselt ka Riigi Infosüsteemi Ameti (RIA) CERT-ini. Seetõttu on meie seisukoht, et pigem tuleks riike suunata välja töötama lahendusi, mis võimaldaksid asjassepuutuvate pädevate asutuste samaaegset teavitamist, mis ühest küljest tagaks koheselt vajaliku info kättesaadavuse, kuid teisalt hoiaks kokku ka teavitaja ressurssi. Näiteks saaks luua teavituskanali, kuhu intsidendiraport ühekordselt sisestatakse ning pädevad asutused saaksid turvaliselt ligi just neile vajalikule intsidenditeabele. Siinkohal tuleb arvestada, et teave, mille vastu pädevatel asutustel on huvi, on erinev. Seetõttu ei ole meil võimalik nõustuda ka ettepanekuga, mille kohaselt edastatakse intsidenditeave kõigepealt Finantsinspektsioonile ja sealt alles omakorda RIA-le, sest esmast teavet küberintsidendi toimumise fakti kohta on RIA-l vaja koheselt. Täna on Eestis näiteks loodud tööriist https://raport.cert.ee, mille kaudu on võimalus teavitada küberintsidentidest korraga nii RIA-t kui Politsei- ja Piirivalveametit (PPA). Analoogselt osundatakse samale tööriistale ka PPA lehel. | |
| | Arvestades, et määrus kehtestab finantssektori-spetsiifilised ühetaolised nõuded IKT süsteemide turvalisusele ning kohaldamisalas on üle 20 teenuseosutaja, kellest paljudele täna küberturvalisuse nõuded ei kehti, suurendab see kindlasti asjaomaste ettevõtete kulusid. Proportsionaalsuse põhimõttest lähtuvalt võiksid olla:<br>a. regulatiivsed leevendused väikestele teenuseosutajatele;<br>b. eeskirjad, mis kohalduvad ainult olulistele teenuseosutajatele;<br>c. eraldi nõuded tegevuse spetsiifikast lähtuvalt, mis on võimalik määratleda siseriiklikult. | |
| | Käesolev arvamus sisaldab Riigi Infosüsteemi Ameti märkusi DORA ettepaneku kohta. | |
| | **MKM-i kommentaarid krüptovarade õigusliku raamistiku osas** | |
| | Oleme selles teemas kriitilise pilguga reguleerimise poolt ning ka riigi/VIK poolt tuleks teha igale taotlejale põhjaliku taustakontrolli, et mis on ikkagi ärimudel enne tegevusloa andmist. Kaaluda seda, et kas tagatiste mahud, alates millest võib tegeleda, võiksid emiteeri-jatele olla kohustuslikud? Kaaluda eeskuju võtmist olemasolevate börsiinstrumentide reeglitest, käsitleda token'eid võlakirjadena vms. | |
| | Toetame eelnõu eesmärki korrastada krüptovarade tururegulatsioone. | |
| | Peame reguleerimisel oluliseks lähtumist eelkõige toimingute sisust, mitte niivõrd nende krüpto või mittekrüpto vormist. | |
| | Leiame, et nõuete kehtestamisel tuleks jälgida otstarbekuse põhimõtet piiritledes regulatsiooniga hõlmatud sihtrühma teenuste skoobi ja mahu osas. | |
| | Eelnõus on põhjalikult käsitletud krüptovaradega seotud teenuse osutamise alustamist, kuid väga lakooniliselt on puudutatud | |

| | | |
|---|---|---|
| | teenuse osutamise lõpetamist. See võib olla Eesti jaoks oluline teema arvestades meil registreeritud vastava valdkonna ettevõtete suurt arvu. | |
| | Eelnõu sisaldab mitmeid viiteid EBA ja ESMA poolt loodavatele tulevastele standarditele. Peame oluliseks, et sisulised nõuded teenuseosutajatele tuleneksid eelkõige õigusaktist, mitte ei selguks 12 kuud peale õigusakti vastu võtmist, kui on tekkinud mainitud standardid. | |
| | Krüptovarade määruse konsultatsiooni raames esitatud küsimused on igati õigustatud ja ka krüptovarasid tuleks määratleda ja defineerida üsna täpselt ehk nii nagu ka praegu sellele lähenetud on, et neid poleks võimalik kuritarvitada.. Samas on tegu keerulise ülesandega, kuna uusi tokeneid tuleb üsna tihedalt juurde. Näiteks täna eksisteerivad ka STO-d (security tokenid), mis peaks lahendama usaldustokenite läbipaistmatuse ja tooma need hallist alast välja, et VKE-sid rahastada. Reaalsuses on STO-d tekitanud veelgi suurema lõhe finantsjärelevalve, raha kaasavate ettevõtete ja investorite vahele. Valdav enamus maailmas, sh Eestis, läbi viidavaid STO-sid on olemuselt väärtpaberite avaliku pakkumise läbiviimise nõudeid eiravad struktureeritud võlakirjade emiteerimised või siis investorite petmine. Eks selle vältimisele aitabki kaasa kui usaldustokenid ja muud tokenid on hästi defineeritud, mille kaudu oleks teoreetiliselt võimalik rakendada ka erinevaid alternatiivseid ja ka läbipaistvaid VKE-de rahastamisviise. | |
| **2** | **Siseministeerium** | |
| | Digirahastuse strateegias toodud eesmärke saame toetada. Eeskätt järgnevat: "Komisjon teeb 2021. aastal osana laiemast rahapesu ja terrorismi rahastamise tõkestamise algatusest ettepaneku ühtlustada klientide registreerimise eeskirju ning tugineb e-IDASe eelseisvale läbivaatamisele, et rakendada digitaalse identiteedi koostalitlusvõimeline piiriülene raamistik." Toetame ka algatust, millega soovitakse määratleda, milliseid isikut tõendavaid dokumente on vaja isikusamasuse kontrollimiseks, ja täpsustada, milliseid tehnoloogiaid võib kasutada isikusamasuse kaugkontrolliks. Vastavat sisu eraldi täpsemalt esitatud materjalid ei käsitle. Seejuures viidatakse eelkõige e-IDAS määruse läbivaatamisele, mille protsessi me samuti panustame. Märgime EE osas, et meie anname välja ka kolmanda riigi kodanikule (kui ka EL kodanikule) kõrge tasemega isikutunnistust, mis saaks olla finantssektorile ligipääsu tagamise vahendiks. | |
| | Tehisintellekti vahendite kasutuselevõtu edendamisega seoses on oluline märkida, et väljatoodud probleemid (tehisintellekti usaldusväärsus ning läbipaistvus, profileerimine ja sellel põhinevad otsused) ei ole omased ainult finantssektorile, vaid on sarnased ka näiteks korrakaitses ja haldusmenetluses tehisintellekti rakendamisel kerkivate probleemidega. Seetõttu tuleks kaaluda pigem üldiste järelevalvesuuniste väljatöötamist tehisintellekti rakenduste kasutamise kohta, mis lähtuksid eelkõige lahenduste riskiastmest ning kasutatavatest andmetest (nt kas kasutatakse isikuandmeid). Täiendavalt sektoripõhiste lisaregulatsioonide kehtestamine võiks olla järgmine samm spetsiifiliste probleemide lahendamisel. | |
| | Muus osas leiame, et paketis ettenähtud digitaalsetele lahendustele ning regulatsioonidele peaks hinnangu andma eelkõige Majandus- ja Kommunikatsiooniministeerium, kes vastutab Eesti digiriigi arengukava koostamise eest. | |
| | **Siseministeerium, olles konsulteerinud valitsemisala allasutustega, edastab finantsteenuste digitaalse operatsioonilise resilientsuse akti** | |

| | | |
|---|---|---|
| | **konsultatsioonidokumendi (DORA) kohta alltoodud tähelepanekud.** | |
| | Arvestades sektori kiiret arengut ning kasvavaid riske, tervitame Euroopa Komisjoni kavatsust töötada välja ühised seadusandlikud ettepanekud virtuaal-/ krüptovarade reguleerimiseks. DORA määruse eelnõu kohaldamisalasse (artikkel 2) kuulub 20 erinevat teenuseosutajat, neist enamuse moodustavad finantsteenuse osutajad (sh krediidiasutused, kindlustusandjad, -vahendajad, investeerimisühingud, fondivalitsejad, ühisrahastusteenuse osutajad jt), lisaks audiitorid ja kolmandatest osapooltest IKT teenuseostajad (edaspidi teenuseosutajad). | |
| | Vastusena Rahandusministeeriumi küsimusele, kas määrus peaks kohalduma kõikidele ettepanekus määratletud teenusepakkujatele leiame, et kuigi ühetaoline lähenemine on oluline, tuleks ka DORA puhul sarnaselt AMLD ülesehitusele määratleda kõrgema riskiga sektorid ning vastavalt riskianalüüsidele arvestada teiste sektorite võimekusega vastata kohaldamisalas reguleeritud nõuetele. Kindlasti tuleks selles määratluses võtta arvesse ka teenusepakkuja laadi.<br>Samuti peaks riskianalüüsile tuginema ka maksesüsteemide välistamine erisusena – sektori välistamine ei või toimuda kergekäeliselt. | |
| | Nimetatud õigusaktide eelnõude peamiseks eesmärgiks finantssektoris esinevaid digitaalsete riskide, sealhulgas küberriske, maandamine ja ennetamine. Nagu on välja toodud ka probleemikirjelduses, on küberkuritegevuse vastase võitluse perspektiivist laiem probleem see, et valdkond ei ole jätkuvalt digitaalset arengut arvestavalt läbivalt reguleeritud. Esiteks on oluline ühiskonna toimepidevus – pakutavad teenused peavad olema turvalised, mille tagamisel on ettevõtetel järjest suurem roll. Ettevõtjate ning teenuseosutajate panustamine küberturbesse peab saama uueks suunaks, mistõttu peaks määrus kohalduma võimalikult laiale turuosaliste ringile. Teiseks tuleb lõplikult reguleerida erinevad virtuaalvaluutadega seonduvad aspektid ning otsustada, kuhu suunas Euroopa Liit tervikuna liigub. Ehk teisisõnu, vastutus, kasutamine, registreerimine, mis on selliste maksevahendite kasutamisel lubatud ja mis mitte. | |
| | Küberohtude ja haavatavuste teavitamis osas (lk 4 küsimus 15) on täna olukord, kus paljud ettevõtted ei jaga teavet (sealhulgas ka politseile), kuna esineb kohatisi kõrvalekaldeid Euroopa Liidu isikuandmete kaitse üldmäärusest (GDPR) ja kardetakse trahve. Näiteks kui ettevõtet tabab küberrünnak, mis toob kaasa klientide andmete lekkimise jms. Odavam on intsidentidest vaikida lootuses, et teave ei jõua avalikkuseni, mis omakorda loob soodsa pinnase järgnevateks rünneteks. Kuivõrd digitaalsed teenused puudutavad väga paljusid kliente (nii era- kui juriidilised isikud) ja nende isikuandmeid, võiks kaaluda kohustamist, kuivõrd küberrisk või rünnak ei puuduta üksnes eraettevõtteid. Kokkuvõtvalt on oluline, et erinevate õigusaktide raames ei oleks eesmärgiks luua uusi asutusi ja mudeleid, vaid integreerida EL õigusruum ühiseks tervikuks, rakendades selleks võimalikult parimal moel olemasolevaid struktuure. | |
| | Euroopa Komisjoni hinnangul tähendab finantssektori järjest suurem sõltuvus tarkvarast ja digitaalsetest protsessidest ka info- ja kommunikatsioonitehnoloogiaga (IKT) seotud riskide kasvu. Politsei- ja Piirivalveameti küberkuritegude üksuse arvates võiks antud teemal siseriiklik pädevus koonduda Riigi Infosüsteemi Ametisse (RIA), | |

| | | |
|---|---|---|
| | kuivõrd taoliste nõuete kehtestamine ning kaasnevate tagajärgede hindamine kuulub eelkõige Majandus- ja Kommunikatsiooniministeeriumi ja/või RIA kompetentsi. | |
| | Krüptoraha puhul tuleb arvestada, et sarnased teenused jäävad eksisteerima. Mõistlik on IKT turbepoliitika ühtlustada, kuna sellega kaitseme ühelt poolt teenusepakkujaid, kuid teisalt ka nende kliente. Kindlasti on oluline, et kui finantsasutused satuvad kuriteo ohvriks, siis neil oleks säilitatud andmed, mida korrakaitseasutused uurimiseks kasutada saavad. Kuna krüptoraha vahendajad on ahvatlevad sihtmärgid, aitab IKT nõuete sätestamine vähendada nii seda tüüpi uurimiste hulka kui tagada menetlemisel vähemalt teatud teabe olemasolu. | |
| | Määruse reguleerimisalasse kuuluvate tegevusvaldkondade ning artiklis 44 nimetatud pädevate asutuste regulatsioon tuleks kujundada selliselt, kus Eestis vastav roll kontsentreeritakse ning välistataks Rahapesu Andmebüroo roll selles, kuivõrd tegemist ei ole AML järelevalvega sobituva ülesandega. | |
| | Põhimõtteliselt toetame IKT-nõuete osas standardite kehtestamist virtuaalvääringute ja ühisrahastuse osas, kuid ei ole pädevad seda regulatsiooni täpsemalt hindama. Eesti vaates oleksid ilmselt vajalikud täiendavad välistusalused määruse kohaldamisalast (mitte virtuaalvääringu teenusepakkujate osas), kuivõrd esitatud nõuded tekitavad osadele teenusepakkujatele (ka mikroettevõtjatest suurematele) ilmselt liialt suure halduskoormuse. | |
| | | |
| | **Finantsinspektsioon** | |
| **3** | Täname võimaluse eest avaldada arvamust Euroopa Komisjoni finantsteenuste digitaalse operatsioonilise resilientsuse määruse (DORA) (edaspidi *Määrus*) ning DORA ja MiCA määrustega kaasneva direktiivi (edaspidi *Direktiiv*) konsultatsioonidokumendi kohta (Määrus ja Direktiiv koos edaspidi *Konsultatsioonidokument*).<br>Käesolevaga esitame Finantsinspektsiooni vastused rahandusministeeriumi poolt koostatud suunavatele küsimustele Konsultatsioonidokumendi osas, mille osas Finantsinspektsioonil on puutumus. | |
| | **Kas Määrus peaks kohalduma kõikidele ettepanekus määratletud teenuseosutajatele? (küsimus nr 3)**<br>Kindlustussektoris ei ole hetkel kolmandatest osapooltest info- ja kommunikatsioonitehnoloogia (edaspidi *IKT*) teenuseosutajad finantsjärelevalve all (näiteks kindlustusmaaklerite ja -seltside vahelise platvormi omanikud või haldajad). Finantsinspektsiooni hinnangul ei ole siiani tekkinud olukordi, kus oleks vajadust kehtestada ettepanekus määratletud teenuseosutajatele ühetaolisi nõudeid IKT süsteemide turvalisusele, kuid me ei välista selle vajaduse tekkimist tulevikus ning seda eriti just suuremate teenuseosutajate osas.<br>Usume, et krediidiandjatest ja -vahendajatest subjektide IKT risk mõneti väiksem võrreldes reaalselt kliendi vara hoidvate krediidiasutuste või makseasutustega. Krediidiandjatest ja -vahendajatest subjektide puhul on eelkõige oluline, et Määruse alusel kehtestatavad uued IKT nõuded ei oleks liigselt koormavad krediidiandjatele ja –vahendajatele kui nn väiksematele subjektidele ning et neil ei oleks Määrusest tulenevate nõuete täitmine ebaproportsionaalselt keeruline. | |

| | | |
|---|---|---|
| | **Kas teie hinnangul ettepanekus esitatud proportsionaalsuse põhimõtted võtavad õiglaselt arvesse teenuseosutaja laadi, organisatsiooni struktuuri ja juhtimist, tegevuse mahtu jne? Kui ei, milliste teenuseosutajate või milliste tegevuste suhtes tuleks ette näha täiendavad leevendused või välistused? (küsimus nr 4)**<br>Olukorras, kus kogu äritegevus kindlustussektoris on muutumas digitaalseks, on proportsionaalsete standardite kehtestamine mõistlik. Finantsinspektsiooni hinnangul tuleks kaaluda, kas kindlustusagentide ning -agentuuride, kui kindlustuse turundamise ühe liigi osas, on mõtet neid allutada Määruse kohaldamisalasse arvestades, et nad tegutsevad kindlustusandja vastutusel ja kasutavad kindlustusandjate süsteeme-programme, mis on allutatud finantsjärelevalve alla. Teeme ettepaneku antud küsimust täiendavalt analüüsida. | |
| | **IKT riskide juhtimine (Määruse artiklid 4-14). Üldine seisukoht ja muud tähelepanekud IKT riskide juhtimise kohta. (küsimus nr 8)**<br>Määruse artikkel 4 lõige 2 osas märgib Finantsinspektsioon, et kuivõrd mikroettevõtted ostavad IKT teenused välistelt teenusepakkujatelt, siis võiks kaaluda nende IKT teenuste osas teenuseosutajatega sõlmitud teenuselepingute järelevalvet.<br>Määruse artikkel 5 lõige 7 osas on Finantsinspektsioon seisukohal, et mikroettevõtted võiksid olla IKT audiitorite poolt teostatavate regulaarsete IKT auditite kohustusest vabastatud. | |
| | **IKT-ga seotud intsidentidest raporteerimine (Määruse artiklid 15-20).** Kas teie hinnangul on selline EL tasandil harmoniseeritud teavitamismudel asjakohane ning seda peaks kohaldama kõikide teenuseosutajate suhtes. Kui mitte, siis miks ja millised on teie ettepanekud eeskirjade parandamiseks? (küsimus nr 9)<br>Finantsinspektsioon on seisukohal, et EL tasandil harmoniseeritud teavitamismudel on asjakohane. | |
| | **Digitaalse operatsioonilise resilientsuse testimine (Määruse artiklid 21-24). Kas DORA IV peatükis sätestatud testimisraamistik on arusaadav? Kui ei, mida tuleks täpsustada või muuta? Kas Eesti peaks implementeerima ka Tiber-EU testimisraamistiku? (küsimus nr 11)**<br>Määruse artikli 23 punkti 2 kohaselt tuleb testi ulatus ja tulemused valideerida pädeva asutuse poolt. Oleme seisukohal, et konkreetse TLPT metoodika kehtestamiseks puudub konkreetne vajadus. Usume, et Tiber-EU testimisraamistiku Eestis implementeerimise vajaduse hindamiseks oleks vajalik sellekohane hinnang turuosalistelt. | |
| | **Üldine seisukoht artiklites 21-24 sätestatud kohta. (küsimus nr 12)**<br>Määruse artikli 23 lõike 2 kohaselt tuleb pädevatel asutustel hinnata TLPT testi kohta esitatud dokumentatsiooni ning väljastada tõend (ingl k *issue an attestation*). Finantsinspektsioon juhib tähelepanu, et Määruses ei ole täpsustatud, mida kõnealune tõend sisaldama peaks ning millist eesmärki ta täidab. Meie hinnangul võiks järelevalve antud osas pidada sisemist registrit, mille abil oleks võimalik tõhusamalt testimisi ning nendega seonduvat dokumentatsiooni hallata. | |
| | **Mida te arvate sellest, et ettepaneku kohaselt teostatakse kriitilise tähtsusega kolmandate osapoolte üle järelevalvet EL tasandil? (küsimus nr 14)**<br>Finantsinspektsioon ei ole vastu, et EL tasandil oluliste ja globaalsete IKT teenusepakkujate osas teostatakse järelevalvet EL tasandil. | |

| | | |
|---|---|---|
| | **Küberohtude ja haavatavusega seotud informatsiooni jagamine (Määruse artikkel 40). Millist lisaväärtust te näete selles, et artikli 40 kohaselt võiksid finantsteenuse osutajad omavahel küberohtude ja haavatavuse kohta (vabatahtlikult) teavet jagada? (küsimus nr 15)**<br>Oleme seisukohal, et laiem infovahetus võimaldab paremini erinevaid nõrkusi ning potentsiaalseid ründekohti tuvastada ning neile rohkem tähelepanu juhtida. Eeltoodu võimaldab igal ettevõttel oma lahendusi viidatud aspektist hinnata ning nõrkused oma süsteemidest kõrvaldada. Usume, et konkreetsel perioodil toimuvate ründetüüpide kohta info parem ja laiem kättesaadavus võimaldab vajadusel kogu sektoril täiendavaid ettevalmistusi teha. | |
| | **Kas te näete selles teavitamises ka ohte või üldisi takistusi? (küsimus nr 16)**<br>Finantsinspektsioon on seisukohal, et juhul kui info jagamine toimub piisavalt üldiselt tasemel ilma tehniliste detailideta, siis ei tohiks teavitamisega kaasneda ülemäära suuri ohtusid ega takistusi. | |
| | | |
| **4** | **Eesti Pank** | |
| | Eesti Panga arvamus Euroopa Liidu digirahanduse strateegia, jaemaksete strateegia ja seotud õigusaktide paketi kohta | |
| | Täname võimaluse eest anda arvamus Riigikantselei algatatud avalikus konsultatsioonis õigusaktide paketi kohta, mis sisaldab ettepanekuid Euroopa Parlamendi ja nõukogu õigusaktide ettevalmistamiseks üldise eesmärgiga reguleerida finantssektori digitaalsete lahenduste usaldusväärset toimimist, hajusraamatu tehnoloogiat ja krüptovarasid. | |
| | 1. Eesti Pank toetab uue Euroopa Liidu õigusraamistiku väljatöötamist krüptovarade, sealhulgas varaga tagatud krüptovarade (stablecoins) ja utility token'ite osas. Mõned big tech ettevõtjad on juba andud avalikkusele sõnumeid, et nad kavatsevad Euroopa turule tuua tagatud krüptovaradel põhinevaid makselahendusi (näiteks Libra), mida aga praegu on veel keeruline kindla regulatsiooniga hõlmata. Et tagada tarbijakaitse nõuete täitmine ning aus konkurents Euroopa makseturul, peavad uued lahendused olema kooskõlas kehtiva õigusraamistikuga, samas peab olema võimalik kohandada ka õigusraamistiku nii et see arvestaks tehnoloogias toimuvate arengutega. Selge regulatsioon loob usaldusväärse taustsüsteemi tehnoloogia arendamisele ja toetab sellega ka innovatsiooni. | |
| | 2. Eesti Pank toetab Euroopa Komisjoni esitatud kava digitaalse vastupidavusvõime ehk DORA määruse vastu võtmiseks, arvestades et määrus kehtestab finantssektori ülesed, sektorispetsiifilised ja võrdsetel alustel nõuded IKT süsteemide turvalisusele ning aitab hoida kõrgel tasemel digitaalsete lahenduste toimimiskindlust. DORA määruse eelnõu käsitleb muu hulgas küberkerksuse testimise nõudeid, mis on põhimõtteliselt kooskõlas Eurosüsteemi küberkerksuse testiraamistikuga TIBER-EU. | |
| | 3. Eesti Pank on huvitatud, et DORA määrusesse kirjutataks selgemalt sisse eurosüsteemi küberkerksuse testiraamistik TIBER-EU ja selle kohaste testide tegemise kord. See aitaks harmoniseerida küberkerksuse testimist ülepiiriliselt ning on kooskõlas ka Eesti Panga strateegilise suunaga tõhustada finantssektori kübervastupanu võimet, mille üks osa on Eesti finantssektorile vastavate testide tegemiseks ühtse raamistiku pakkumine. | |

| | | |
|---|---|---|
| | Kirjale on lisatud Euroopa Komisjoni kahe dokumendi tekstid vastavalt digirahanduse ja jaemaksete strateegia kohta koos kommentaaridega, mis väljendavad Eesti Panga seisukohti dokumentides käsitletud üksikküsimustes. | |
| | **Digirahanduse strateegia** | |
| | Eesti Pank toetab Euroopa Komisjoni eesmärke AML/CFT vallas ja e-IDAS regulatsiooni ülevaatamise osas. e-IDASe osas on Eesti Pank andnud järjepidevalt välja sõnumeid, milles tuuakse välja see, et Euroopal peavad olema hästitoimivad digitaalse identiteedi ja e-Allkirja teenused, mis töötaksid lisaks avalikule sektorile ka kogu finantssektoris. EL peaks rakendama õigusraamistiku, mis võimaldaks koostalitlusvõimeliste digitaalse identiteedi lahenduste kasutamist moel, mis võimaldaks uutel klientidel kiiresti ja hõlpsalt finantsteenustele juurde pääseda. Selleks peab eurosüsteem alustama koostööd turu sidusrühmadega, et töötada välja finantssektorile sobiv tehniline lahendus, mis võimaldab kasutada digitaalse identiteedi ja e-allkirja lahendusi, mis oleks algus laiemate kliendisuhete ja äriprotsesside digiteerimise ja automatiseerimise suunas. Ühtlasi on Eesti Panga seisukoht, et liikmesriikides kasutusel olevad lahendused peaksid jääma kasutusse ning ei tohiks võtta eesmärgiks seda, et Euroopa hakkab looma uut e-ID/e-Allkirja lahendust. Eesti ID-kaart, Mobiili-ID ja Smart-ID peavad jääma kasutusse ja saavutama üleeuroopalise ulatuse. | |
| | Eesti Pank toetab Euroopa Komisjoni uue Euroopa Liidu õigusraamistiku väljatöötamist krüptovarade, sealhulgas varaga tagatud krüptovarade (*stablecoins*) ja *utility token'ite* osas. Teatavad tehnoloogia hiiud on andud avalikkusele sõnumeid, et nad kavatsevad Euroopa turule tuua tagatud krüptovaral põhinevaid makselahendusi (Libra), mida praegusel hetkel on keeruline kindlasse regulatsiooni paigutada. Selleks, et säiliksid tarbijate kaitseks seatud tingimused ning aus konkurentsisituatsioon Euroopa makseturul, peavad makselahendused olema kooskõlas kehtiva õigusraamistikuga ning ka õigusraamistiku peab vajadusel kohandama selliseks, mis arvestaks tehnoloogiliste arengutega. Ühtlasi aitaks selgesõnaline regulatsioon tehnoloogiat edasi arendada ja seeläbi toetada innovatsiooni. | |
| | Eesti Pank toetab komisjoni eesmärki muuta ELi õigusakte, et tagada avalikustatud teabe kättesaadavus standardiseeritud ja masinloetavas vormingus, kui see aitaks kaasa andmetepõhisele innovatsioonile Euroopa Liidus. Reaalajas digitaalse juurdepääsu hõlbustamine kogu reguleeritud finantsteabele, uuenduslike IT-vahendite edendamine aruandluse ja järelevalve hõlbustamiseks, ettevõtetevahelise andmete jagamise edendamine EL-i finantssektoris võivad anda Euroopa majanduse konkurentsivõimele märkimisväärse tõuke ning vastava algatusega peaks jätkama. | |
| | Eesti Panga strateegiline ülesanne on tõhustada finantssektori kübervastupanu võimet pakkudes Eesti finantssektorile välja eurosüsteemis välja töötatud ühtne kübertestimise raamistik TIBER-EU.<br>Seetõttu Eesti Pank toetab Euroopa Komisjoni poolt loomisel oleva DORA määruse (REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations) vastuvõtmist, kuna määrus kehtestab finantssektori üleselt sektori-spetsiifilised ühetaolised nõuded IKT süsteemide turvalisusele, tagades | |

| | | |
|---|---|---|
| | kõrgtasemelise digitaalse operatsioonilise resilientsuse. DORA määruse eelnõu käsitleb muu hulgas küberkerksuse testimise nõudeid ning määruse eelnõus olev ohuteabel põhineva testimise nõue, väliste osapoolte kasutamine jm on põhimõtteliselt kooskõlalised Eurosüsteemi küberkerksuse testiraamistikuga TIBER-EU.<br>**DORA määruse näol kogu finantssektorile ühtlustatud baasnõuete kehtestamine on selgust loov eesmärk. DORA määrus peaks finantssektori kriitiliste infrastruktuuride küberkerksuse testimise osas andma selgeid viiteid ja seoseid eurosüsteemiülesele küberkerksuse testiraamistikule TIBER-EU**. See aitaks harmoniseerida kübertestide tegemise üle Euroopa ning annaks pädevatele asutustele võimaluse testitulemusi valideerida. | |
| | **Jaemaksete strateegia** | |
| | Eesti Pank toetab SEPA välkmaksete kasutuselevõttu (laialdaselt ja kõigis pangakanalites). Eesti Pank on seisukohal, et lõpptulemusena võiks SEPA tavamaksed täielikult SEPA välkmaksetega asendada.<br>Eestis on välkmaksete osakaal 61% pankadevahelistest maksetest (sept 2020). SCT inst on skeemiga EPC info kohaselt liitunud 6 turuosalist (4 suurpanka, TBB ja Pocopay), SCT skeemiga 11. Eesti on välkmaksete kasutuselt Euroopas esimene ja välkmaksete tegemise võimalus on enamikul pangaklientidel (96% kontodest on välkmaksevõimalusega). Mujal Euroopas välkmakseid nii laialdaselt ei kasutata ja ilmselt ei suudeta täita nõuet, et novembris 2020 peab enamik turuosalistest olema SCT inst skeemi kasutusele võtnud. Ka Eesti puhul peab möönma, et nõude täitmine sõltub kasutatavast metoodikast. | |
| | Eesti Pank toetab vajadust hinnata, kas on asjakohane nõuda SEPA välkmaksete pakkumiseks täiendava funktsionaalsuse kasutamist ja teha selleks ettekirjutusi. Eesti Pank toetab ka vajadust täiendavate standardite loomiseks. Eesmärk on saavutada välkmakselahenduste koostoime ja standardiseerimine on selleks üks lahendus. | |
| | Hoolikalt tuleks järgida järgmiste teemade arengut:<br>1) tarbijate kaitsemeetmete täiendamine SEPA välkmaksete suuremaks kasutamiseks (Pillar 1, punkt 2 Increasing consumers' trust in instant payments)<br>2) SEPA potentsiaali täielik kasutamine SDD osas (Pillar 1, punkt 4 Reaping the full potential of the Single Euro Payments Area (SEPA)) | |
| | Eesti Pank toetab Euroopa Komisjoni nägemust muuta välkmaksed nn. uueks normaalsuseks ning hindamaks põhjuseid, mis takistavad selle nägemuse saavutamist. Küll aga me ei toeta tagasinõude õiguse laiendamist välkmaksetele, sest need on olemuslikult kreeditkorraldused, millele ei rakendata tagasinõudeõigust. Sarnase tagasinõude kehtestamine nagu SEPA otsekorraldustel tooks kaupmeestele ja ka eraisikutele kaasa ebakindluse ootamatute makse tagasinõuete näol. Selle asemel ja välkmaksete turvalisuse kasvatamiseks toetab Eesti Pank üleeuroopalise makse saaja nime ja kontonumbri kontrolli lahenduse loomist ning kasutamist enne makse kinnitamist. | |
| | Eesti Pank toetab Euroopa Komisjoni eelloetletud tegevussuundasid sh kaupmeeste, eelkõige väikeettevõtete makselahenduste täiendamist ja lihtsustamist ning nende teadlikkuse suurendamist. Lisaks toetab Eesti Pank makseahela täielikku digitaliseerimist alustades üleeuroopalistest e-arve (ja request-to-pay) makselahendustest ning lõpetades e-kviitungitega. Üleeuroopalise ulatusega Euroopa valitsemise ja brändiga makselahendus vähendab sõltuvust globaalsetest | |

| | | |
|---|---|---|
| | kaardiskeemidest. Ühtlasi suudaks üleeuroopaline makselahendus konkureerida erinevate globaalsete tehnoloogiaettevõtete (Facebook, Google, Amazon, Apple) vastavate lahendustega.<br>Eesti Pank viis 2020. aasta suvel väikeettevõtete seas läbi küsitluse, mille eesmärk oli saada teada, kas ettevõtjad on huvitatud makselahendusest, mis võimaldab neil oma toodete või teenuste eest kohe näiteks pangaäppi või QR-koodi teel raha küsida ning saada tasu välkmaksena. Uuringust selgus, et väikekaupmehed ootavad väga võimalust saada makseid ilma kaardimakseks vajalikku taristut omamata - 76% vastanutest tõid välja, et nad tunneksid uue makselahenduse vastu huvi, kui see oleks soodne, tarbijale mugav ja tagaks raha kiirema laekumise.<br>Maksekeskkonna arendamise küsimusi arutab Eesti Pank turuosalistega koostöös regulaarselt. Digitaliseerimise ja uuendamise nimel hakkab tegutsema ka äsja Maksekeskkonna Foorumi alla loodud maksekeskkonna digitaliseerimise töögrupp. | |
| | Eesti Pank toetab SEPA määruse täitmise jälgimist. IBAN diskrimineerimine ei ole Eesti Pangale teadaolevalt Eestis aktuaalne. Seetõttu oleme sel teemal neutraalsed. Samas tuleb tõdeda, et Eesti pangad ei ole SDD skeemiga liitunud ja ei paku üleeuroopalise otsekorralduse teenust. Eesti maksekeskkonna toimimist see ei takista, sest Eestis kasutatakse SEPA otsekorralduse asemel e- arve püsimakseteenust, mis tugineb SEPA kreeditkorralduse skeemile. SEPA otsekorralduse mittepakkumine võib kaasa tuua selle, et Eesti pangakonto omanikud ei saa välismaise teenusepakkuja juures tema pakutavat SEPA otsekorraldust kasutada. | |
| | Eesti Pank toetab siseriiklike eID ja eAllkirja lahenduste üleeuroopalist tunnustamist ja kasutamist finantssektoris ja eIDAS asjakohastamist. Eestis peame seisma selle eest, et finantssektor hakkaks tunnustama ja lubaks kasutada piiriüleseid e-identiteete ja eAllkirju. Eesti Pank ei toeta uue nö „Euroopa lahenduse“ loomist, vaid sooviks koostalitlust võimaldavat süsteemi, mis võimaldaks kasutatada nii ID-kaardi, Mobiili-ID kui ka Smart-ID lahendusi kõikjal Euroopas. | |
| | Eesti Pank toetab eletrooniliste maksete kasutamise uuringu läbiviimist sh väikeettevõtetes ja avalikus sektoris. Eestis on maksekeskkond pigem elektrooniline. Seetõttu ei näe me vajadust elektrooniliste maksete kasutamise võimalikuks reguleerimiseks. | |
| | Eesti Pank toetab algatusi, mis on suunatud euro sularaha kättesaadavuse tagamiseks ning kindlustavad, et euro pangatähed ja mündid on tarbijate ja kaupmeeste poolt eelistatud maksevahendiks. Eesti Pank propageerib maksekeskkonda, kus saab kasutada erinevaid makseviise ning ühiskonnas oleks alternatiivne lahendus, kui üks või teine maksesüsteem ei tööta. Enne konkreetsete meetmete kasutusele võtmist pooldame põhjaliku analüüsi koostamist eesmärgiga selgitada välja sularaha vastuvõetavust ning kättesaadavust piiravad tegurid et kavandatavad meetmed oleksid võimalikult mõjusad. | |
| | Eesti Pank toetab Euroopa Komisjoni soovi teha EKPga koostööd keskpanga digiraha teemal. Eesti Pank osaleb aktiivselt eurosüsteemi vastavates aruteludes ja praktilises testimises. Eesti Pank panustab eurosüsteemi keskpanga digiraha analüüsimisse vedades uurimisprojekti selgitamaks, kas Eesti e-riigi alustehnoloogia *KSI plokiahel* võimaldab digiraha luua/kustutada, seda opereerida, arendada sellele mugavaid lahendusi. | |

| | | |
|---|---|---|
| | Eesti Pank toetab PSD2 mõjude hindamist ja direktiivi ülevaatamise vajalikkust. Eesti Pank toetab avatud panganduse ligipääsu (API) liidese üleeuroopalise standardi ja ühtse rakendamise skeemi (reeglistiku) väljatöötamist. Eestis on võimalik kasutada nii kontoinfo- (AIS) kui ka maksealgatusteenust (PIS), mis mõlemad põhinevad avatud pangandusel. Kontoinfoteenuse puhul on võimalik siduda omavahel mitme panga kontod, nii et ühele kontole sisse logides on võimalik näha ka teise konto vahendeid. Maksealgatusteenuse näiteks on universaalne pangalink. | |
| | Eesti Pank toetab makseteenuste turvalisust tugevdavate meetmete rakendamist ning Euroopa Komisjoni poolseid samme meetmete rakendamise jälgimiseks.<br>Eesti Pank toetab tugeva autentimise nõude (SCA) rakendamine vajalikkust. 31. detsembril 2020 jõustub kaarditehingutele tugeva autentimise nõue ning kõikide e-poodide kaardimakselahendused peavad põhinema uuel 3-D Secure protokollil. 2020 viimased statistilised näitajad SCA osas näitavad, et Eestis on tugevalt autenditud kaardiga tehtud e-ostude osakaal Euroopa keskmisega võrreldes samal tasemel, samas puudub meil praegu analüüs, kui suur osa tugevalt autentimata tehingutest liigituvad erandite alla. Oleme võtnud teema fookusesse<br>Eesti Pank toetab ka Euroopa Komisjoni poolset analüüsi küsimuses, kas maksja nime ja IBANi kokkulangevuse kontroll aitab kaasa pettuste vähendamisele.<br>Et makseteenusepakkujad oleksid võimelised end küberrünnakute eest kaitsma, sel eesmärgil toetab Eesti Pank Euroopa Komisjoni eelnõu DORA vastuvõtmist ning sidumist eurosüsteemi küberkerksuse testiraamistikuga TIBER-EU. Lisaks analüüsime Eesti finantssektorile TIBER raamistiku pakkumise vajadust. | |
| | Eesti Pank toetab kontaktivabadele maksetele kehtivate õiguslike piirangute ülevaatamist selleks, et leida tasakaal mugavuse ja pettuse ohu vahel. Omalt poolt saame kaasa aidata pressiteadete/blogiartiklitega, mis on suunatud inimeste teadlikkuse tõstmisele. | |
| | Eesti Pank toetab Euroopa Komisjoni tegevussuundasid.<br>E-raha direktiivi muutmise juures soovitame paralleelselt tähelepanu hoida SFD uuendamisel. Nimelt SFD uuendamise üheks eesmärgiks on mittepankadele (e-raha asutused ja makseasutused) otsese ligipääsu võimaldamine jaemaksesüsteemidele. Kuna aga sellise võimaluse tekitamine võib kaasa tuua täiendavad riskid jaemaksesüsteemidele, siis võimalike riskide katmine võiks toimuda juba e-raha direktiivi tasandil.<br>Taustainfoks, et eurosüsteemi PISA järelevaatamise raamistik kirjeldab põhimõtted, mis osas ja viisil järelevaatajad ning järelevalvajad saavad koostööd teha PISA raamistiku kohaldusalas olevate skeemide jarelevaatamisel/valvamisel. PISA raamistik kohaldub makseskeemidele nagu kreeditkorraldused, otsekorraldused ja kaardimakseskeemid ning samuti innovaatilistele makselahendustele ja –korraldustele nagu *stablecoin* lahendused. | |
| | Eesti Pank toetab Euroopa Komisjoni soovi laiendada jaemaksesüsteemide otseselt ligipääsetevate asutuste skoopi e-raha asutustele ja makseasutustele. Ligipääsetavuse laiendamine annab võimaluse kohelda turuosalisi võrdväärselt ning kasvataks arveldusturul konkurentsi, millest võidaksid lõpptarbijad. Täiendavate õiguste andmisel tuleb tuvastada ja katta uute otseste osalejate (e-raha asutuste ja makseasutuste) kõikvõimalikud riskid ning | |

| | | |
|---|---|---|
| | süsteemioperaatorite vajadusega olla kooskõlas neile kehtestatud järelevaatamise nõuetega. | |
| | Eesti Pank toetab Euroopa Komisjoni kavatsust analüüsida, kas on asjakohane teha ettepanek õigusaktide muutmise kohta, mille eesmärk oleks tagada juurdepääs makseteenuste osutamiseks vajalikule tehnilisele infrastruktuurile (nt mobiilseadmete NFC). Üheks kõnealuseks näiteks on Apple'i seadmed, mis piiravad NFC funktsionaalsuse kasutamist neile teenusepakkujatele, mis pole Apple lepingulised partnerid. See tähendab, et Apple soovib saada tasustatud iga makse pealt, mis sooritakse Apple seadmega. | |
| | Eesti Pank toetab ideed, et välkmaksete süsteemid liidestuksid kas TIPSi või RT1ga. Vastava algatuse idee seisneks erinevate süsteemide koostoimivuses, tarbijate rahulolus ning üleeuroopalise välkmaksete ulatuse saavutamises. Samuti toetab Eesti Pank kolmandate riikide liitumist TIPSi või RT1ga, kui süsteemi hoolsusnõuded on täidetud ning rahapesutõkestamise ja terrorismi rahastamise riskid on maandatud. | |
| | **Vastusena Rahandusministeeriumi konsultatsioonidokumendile finantsteenuste digitaalse operatsioonilise resilientsuse akti (DORA) kohta, esitab Eesti Pank lisas 1 oma vastused saadetud küsimustikule.** | |
| | 1. Milline on teie üldhinnang määruse eesmärkidele?<br>Vastus: Antud punktid on kaetud erinevate standardite ja seadustega. ISO27000 perekonna standardid, suuremahulistest intsidentidest teavitamist reguleerib täna Küberturvalisuse seadus, Hädaolukorra seadus ja FI regulatsioonid, EBA suunised, SSM järelevalve. Lisaks on eurosüsteemis välja töötatud küberkerksuse ootused CROE raamistik (Cyber Resilience Oversight Expectations). Samuti on Euroopa Keskpanga poolt välja pakutud ühtne küberkerksuse testiraamistik TIBER-EU. Nimetatute rakendamine kogu sektori vaatest on killustatud, rakendatud ainult osadele kriitilist teenust pakkuvatele institutsioonidele. Seega, kuigi määrusega planeeritav on osaliselt juba reguleeritud, siis EP hinnangul, kogu sektorile ühtlustatud baasnõuete kehtestamine määruse näol on pigem positiivne ja selgust loov eesmärk. Oluline on järgida proportsionaalsuse põhimõtteid. | |
| | 3. Kas määrus peaks kohalduma kõikidele ettepanekus määratletud teenuseosutajatele ?<br>Vastus: Vastuväited määruse artikkel 2 toodud kohaldamisala kohta puuduvad. Mis puudutab kolmandatest osapooltest teenuseosutajaid, siis üldine seisukoht on see, HOS kohaste kriitiliste teenuste osutamiseks kasutatavad kolmandad osapooled (teenusepakkujad) oleksid allutatud ITK nõuetele. Proportsionaalsuse põhimõtete rakendamine on vajalik. | |
| | 4. Kas teie hinnangul ettepanekus esitatud proportsionaalsuse põhimõtted võtavad õiglaselt arvesse teenuseosutaja laadi, organisatsiooni struktuuri ja juhtimist, tegevuse mahtu jne? Kui ei, milliste teenuseosutajate või milliste tegevuste suhtes tuleks ette näha täiendavad leevendused või välistused?<br>Vastus: Nõus | |
| | 5. Kas erisused määruse kohaldumisalas, nt maksesüsteemide välistamine, on teie hinnangul põhjendatud?<br>Vastus: Maksesüsteemide välistamise osas: maksesüsteemid on järelevaadatavad keskpankade poolt ja allutatud keskpanga sätestatud riskide maandamise nõuetele. Nõus sellega, et vältida tuleb | |

| | | |
|---|---|---|
| | dubleerivaid nõudeid. Riigi siseselt koostöö pädevate asutuste vahel (Finantsinspektsioon, RIA, Eesti Pank), aitaks dubleerimist vältida. Eesti vaatest ei oleks maksesüsteemide välistamine vajalik, Euroopa vaate kohta hinnanguid ei anna. | |
| | IKT riskide juhtimine (art 4-14)<br>7. (Ainult turuosalistele) Kuidas on IKT riskide juhtimine korraldatud teie organisatsioonis täna ja kui palju ümberkorraldusi te peaksite tegema käesoleva ettepaneku valguses, sh seoses täiendava personali kaasamise ja investeeringutega IT lahendustesse?<br>Vastus: Küsimus ei kohaldu EP-le, kuna EP ei ole turuosaline. | |
| | IKT-ga seotud intsidentidest raporteerimine (art 15-20)<br>Ettepaneku kohaselt peab teenuseosutajal olema juhtimisprotsess IKT-ga seotud intsidentide monitoorimiseks ja säilitamiseks, misjärel tuleb need klassifitseerida ja olulisematest pädevat asutust teavitada.<br>9. Kas teie hinnangul on selline EL tasandil harmoniseeritud teavitamismudel asjakohane ning seda peaks kohaldama kõikide teenuseosutajate suhtes. Kui mitte, siis miks ja millised on teie ettepanekud eeskirjade parandamiseks?<br>Vastus: Täna raporteerivad krediidiasutused mitmete regulatsioonide alusel, HOS, KÜTS, EBA suuniste ning ka SSM regulatsiooni alusel, intsidentide juhtimisprotsess on kehtestatud ja täiendavat reguleerimist ei oleks vaja. Näeme, et sektoriüleselt ühtlased nõuded raporteerimisele on pigem positiivne. | |
| | Digitaalse operatsioonilise resilientsuse testimine (art 21-24)<br>11. Kas DORA IV peatükis sätestatud testimisraamistik on arusaadav? Kui ei, mida tuleks täpsustada või muuta? Kas Eesti peaks implementeerima ka Tiber-EU1 testimisraamistiku?<br>Vastus: Testiraamistik on arusaadav. Määrusega kehtestatav (ohuteabel põhineva testimise nõue, väliste osapoolte kasutamine jm) on põhimõtteliselt kooskõlaline Eurosüsteemi küberkerksuse testiraamistikuga TIBER-EU. Määruse kohaselt tuleb finantssektori ettevõtete küberkerksuse testid kooskõlastada ja valideerida pädeva asutuse poolt, mis on EP vaatest samuti positiivne. Eesti Pank on võtnud eesmärgiks pakkuda Eesti finantssektorile välja testimisraamistik TIBER-EU. Eesti Tiber-EU raamistiku rakendamise vajaduse väljaselgitamiseks on vajalik kahtlemata diskuteerida /küsitleda Eesti finantssektori turuosalisi. Määrusega kehtestatu kõrval annaks TIBER-EU veel konkreetsema testi metoodika määruse nõuete täitmiseks. Juhul, kui määrus saab kehtestama pädeva asutuse kohustuse finantssektori teste valideerida (nii nagu ettepanekus on öeldud), siis täidaks TIBER-EU ka seda ülesannet, et valideerimine oleks oluliselt lihtsam, kui testid on korraldatud tsentraalselt, ühetaoliselt ja võrreldavalt. | |
| | Kolmandatest osapooltest IKT teenuseosutajatega seonduvad riskid (art 25-39)<br>13. (Ainult turuosalistele) Kas te ostate sisse IKT teenuseid? Kas ettepanekus esitatud lahendused pigem lihtustavad kolmandate osapooltega suhtlemist/läbirääkimisi/lepingu sõlmimist või muudavad selle pigem keerulisemaks?<br>Vastus: Küsimus oli ainult turuosalistele, EP ei ole turuosaline. | |
| | Küberohtude ja haavatavustega seotud informatsiooni jagamine (art 40) | |

| | | |
|---|---|---|
| | 15. Millist lisaväärtust te näete selles, et artikli 40 kohaselt võiksid finantsteenuse osutajad omavahel küberohtude ja haavatavuste kohta (vabatahtlikult) teavet jagada?<br>Vastus: Küberohtude ja haavatavuste kohane täiendav info jagamine aitab kogu sektoril paremini valmistuda küberrünnakuteks ning ka rünnakut tuvastada. Sektori ülene infovahetus, üksteiselt õppimine on ka üks TIBER-EU testiraamistiku aluspõhimõtetest. EP vaates toetame finantssektori spetsiifilise infojagamiskeskkonna loomist. | |
| | 16. Kas te näete sellises teavitamises ka ohte või üldisi takistusi?<br>Vastus: Ohte aitab elimineerida osapoolte vahel sõlmitav koostöökokkulepe (lepped), kus määratletakse info jagamise tingimused. | |
| | Pädev asutus (artiklid 41-49)<br>18. Üldine seisukoht artiklites 41-49 sätestatu kohta.<br>Vastus: Pädeva asutuse kohased artiklid, hetkel seisukoht puudub. | |
| | Delegeeritud aktid, ülevaatusklausel, muudatused muudes õigusaktides ja jõustumisaeg (artiklid 50-56)<br>19. Üldine seisukoht artiklites 56-59 sätestatu kohta?<br>Vastus: puudub | |
| | LISA 2. DORA ja MiCA määrustega kaasnev direktiivi eelnõu, millega muudetakse järgmiseid õigusakte: 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341 Direktiivi eelnõu (edaspidi eelnõu) eesmärk<br>Direktiivi eesmärk on viia olemasolevad Euroopa Liidu õigusaktid kooskõlla DORA ja MiCA nõuetega.<br>1. Üldine seisukoht eelviidatud direktiiviga kavandatavate muudatuste kohta ja võimalikud muud tähelepanekud. Vastus: hetkel puuduvad | |
| | | |
| **5** | **Eesti Pangaliit** | |
| | Täname Teid võimaluse eest avaldada arvamust finantsteenuste digitaalse operatsioonilise resilientsuse akti (DORA) osas. | |
| | Küsimus 1-2. Määruse eesmärgid on üldiselt arusaadavad. Kuid põhjused, miks juba ülereguleeritud sektorile täiendavaid nõudeid produtseeritakse, ei ole arusaadavad. Eriti olukorras, kus alles 30.06.2020 jõustusid nõuded finantsjärelevalve subjekti infotehnoloogia ja infoturbe korraldusele. | |
| | Küsimus 3. Jah, vastuväiteid subjektide ringi osas ei ole. | |
| | Küsimus 4. Jah. | |
| | Küsimus 5. Põhjendused ei ole meie hinnangul piisavalt selgelt välja toodud. | |
| | Küsimus 6. Kohaldamisala on piisav, kuid suure tõenäosusega tekivad probleemid järelevalve teostamisega. Sealhulgas järelevalve korraldamine saab olema keeruline juba ainuüksi laiast subjektide ringist tulenevalt. | |
| | Küsimus 7. Pankade IKT riskide juhtimine on korraldatud täna vastavalt parimale praktikale ja kooskõlas kehtivate regulatsioonidega. Ümberkorralduste osas oleks vajalik analüüs, mida ei ole veel teostanud. | |
| | Küsimus 8. Riskide juhtimine ei ole regulatsioonidest sõltuv, vaid lähtub vajadusest tagada osutatavate teenuste toimepidevus ja piisav reageerimiskiirus muutuvas keskkonnas. Seega regulatsiooni | |

| | | |
|---|---|---|
| | eesmärgiks saab olla üldnõuete kehtestamine, riskipõhise lähenemise ja hea riskijuhtimise tava propageerimine ja järgimise nõudmine. | |
| | Küsimus 9-10. Turuosalised on äärmiselt huvitatud intsidentidest teavitamise mudeli harmoniseerimisest, eriti teavitamismudeli muutmiseks mudeliks, kus oleks välistatud intsidentidest topelt teavitamine eri ametkondadele. Praktiline vajadus on tagada, et IKT valdkonna intsident, mis liigitub üheaegselt küber-, andmekaitse, op. riski intsidendiks jne oleks raporteeritud võimalikult ühetaoliselt, selgelt ja soovitatavalt ühele asutusele. | |
| | Küsimus 11-12. Jah, Eesti peaks Tiber-rakendama. Soovitame sõna „*resilientsus*“ asemel kasutada eestikeelset sõna „*kestlikkus*“. Testimisraamistik on arusaadav ja pooldame selle rakendamist. | |
| | Küsimus 13-14. Antud ettepanekus esitatud lahenduste mõju kolmandate isikute suhtes selgub praktika käigus. Hetkel ei ole võimalik seda prognoosida. | |
| | Küsimus 15-17. Leiame, et see on positiivne algatus, kuid segaseks jäävad siinkohal andmekaitse üldmääruse kohaldamisega seotud küsimused ja võimalikud vastuolud. | |
| | Küsimus 18. Turuosaliste jaoks ei muutu antud ettepanekuga seoses midagi. | |
| | Küsimus 19-20. Leiame, et 12 kuud on piisav aeg. | |
| | Küsimus 21. Juba praegu on antud valdkonnas pankadel vajalik täita erinevaid EL regulatsioone, lisaks kohalik seadusandlus jne. Kui otstarbekas on selles valguses regulatsioonide pidev muutumine ja uute regulatsioonide väljatöötamine? | |
| | | |
| **6** | **ITL** | |
| | Arvamuse esitamine finantsteenuste digitaalse operatsioonilise resilientsuse akti (DORA) kohta<br>Täname Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu (edaspidi ITL) kaasamise eest finantsteenuste digitaalse operatsioonilise resilientsuse (DORA) konsultatsiooni.<br>Arvestades materjali mahukust ja tagasiside andmise lühikest perioodi, jõudsime me analüüsida ainult ettepanekut kehtestada järelevalveraamistik teenusepakkujatele (näiteks kõrgtehnoloogia ettevõtjad ehk Big Techs), kes pakuvad finantsasutustele pilvandmetöötlust või mõnda muud olulist teenust. Seoses sellega teeme ettepaneku jätta info- ja kommunikatsiooni teenuse pakkujatele mõeldud reeglid määrusest välja, et vältida järjekordsete sektorspetsiifiliste reeglite teket. | |
| | Juhime tähelepanu, et Euroopa Komisjon on hetkel üle vaatamas võrgu- ja infosüsteemide turvalisuse direktiivi 2016/1148 (NIS direktiiv). Muuhulgas analüüsitakse, kas laiendada selle kohaldamisala. ITL on seisukohal, et kattuvat ja dubleerivat regulatsiooni tuleb vältida. Kui on otsustatud, et NIS direktiiv on horisontaalne õigusakt, mis reguleerib võrgu- ja infosüsteemide turvalisust, siis peavad vastavad reeglid olema kirjas selles õigusaktis. Järjekordsed sektorspetsiifilised nõuded tekitaksid praktikas segadust. Ettevõtete halduskoormust tuleb vähendada ning regulatsioonides orienteerumine tuleb teha lihtsamaks. | |
| | Seega ei toeta ITL järjekordsete sektorspetsiifiliste küberturvalisuse nõuete kehtestamist DORA-s ning pooldab ühtseid horisontaalseid reegleid. Juhul, kui nähakse vajadust sektorspetsiifiliste reeglite järgi, siis tuleb vastavad ettevõtted NIS-direktiivi kohaldamisalast välja | |

| | | |
|---|---|---|
| | arvata. Iga ettevõtte peab teadma, milline õigusakt tema tegevust reguleerib ja tal peab olema üks kontaktpunkt, kellele ta peab teavitama intsidentidest.<br>Loodame, et leiate võimaluse arvestada meie seisukohta. | |
| | | |
| **6** | **Rahapesu Andmebüroo** | |
| | **Tagasiside krüptovarade määruse kohta** | |
| | **<u>1. Tagasiside krüptovarade määruse kohaldumisala kohta</u>**<br><u>1.1. Kas teie arvates on määruse eelnõu (edaspidi määrus) kohaldamisalasse jäävad instrumendid ja nende liigitus (kõikvõimalikud token'id, sh kasutustoken'id (utility tokens) ja varapõhised tokenid (asset-referenced token) ja e-raha tokenid) põhjendatud?</u><br><br>Määruse eelnõu kohaldamisalas olevad instrumendid on erinevad Eestis praktikas kasutusel olevatest mõistetest ning kehtivatest põhimõtetest. Lisaks erinevad need ka teatud ulatuses eelmisel aastal Rahandusministeeriumi läbiviidud krüptovarade reguleerimise väljatöötamiskavatsusest, mis kasutas teistsuguseid mõisteid nagu investeerimistoken, maksetoken ja kasutus token. Praktikas on siiski oluline erinevaid tokeneid eristada, et tagada just selle tokeniga seonduva riski, ohu ja nende praktikas avaldumist maandav regulatsioon. Siinjuures on oluline väga täpselt eristada tokenite eristamise põhimõtted, sest ainuüksi mõiste kaudu ei pruugi see võimalik olla (tokenid võivad käituda nii ühe, kui teisena). Arvestades, et sektor vajab ühest lähenemist ning asjakohast reageerimist on põhjendatud kõikide tokenite reguleerimine, küsitav on regulatsiooni ulatus ning meetmed, mida ühe või teise teenuse pakkumisel kohaldama peab – näiteks puudub selge arusaam, kuidas tuvastatakse asjaolu, kas krüptovara on pakutud vähemale kui teatud arvule isikutele või kas avalikkusele pakutava krüptovara hulk ületab teatud summat, seda tuleks hinnata ka lähtudes erinevate regulatsioonide kohaldumise erisusi ning erinevaid aluseid regulatsiooni kohaldumisest. Sellise arvestuse tagamiseks peaks kõikidel liikmesriikidel olema kohene ligipääs kõigi teiste liikmesriikide vastavatele andmetele, mida praktikas ei ole. Kokkuvõtvalt on tokenite eristus oluline ja vajalik. Arvestades, et ka varasemalt on lähenemine tokenite osas olnud sarnane, siis ei ole põhjust seda teistsuguselt koostada, aga oluliseks saab kuidas nõuded erinevatele tokenitele erinevad ning kuidas tokeneid eristatakse, kui see olemuslikult vastab mitmele tokeni liigile. | |
| | <u>1.2. Kas määruse kohaldamisala tuleks siiski muuta/piiritleda ja määratleda määruse kohaldumisalasse kuuluva krüptovara vormi nii, et see oleks seotud eelkõige finantstulu teenimisega ja/või investeerimisriskiga?</u><br><br>Euroopa Liidu eesmärk krüptovarasid reguleerida peaks olema võimalikult laiapõhjaline. See tähendab, et regulatsiooniga tuleks sätestada peamised põhimõtted kõiki krüptovarasid arvestades ning reguleerides, aga nõustume, et kõikide krüptovarade osas ei peaks olema regulatsioon ühetaolise ülesehitusega. Näiteks finantstulu/ investeerimisriski mitte kandvate tokenite reguleerimine peaks olema eristuv e-raha ja varapõhistest tokenitest (hetkel artikkel 4 kaudu on lähenemine üsna ühetaoline, erinedes vaid tingimuste osas). Sõltumata eelnevast peab regulatsioon olema piisav, et välistada selliste tokenite osas hilisemalt praktikas võimaluse tekkimine, et neid kasutatakse/pakutakse siiski finantsriski sisalduvalt (juhul, kui regulatsioon katab probleemid osaliselt üritatakse regulatsiooni alt välja | |

| | | |
|---|---|---|
| | jäänud osa edasi arendada või tõlgendada, et see jääks regulatsioonist välja, aga võimaldaks finantstulu teenida või sisaldaks investeerimisriski). | |
| | 1.3. Kas teie arvates on e-raha direktiivis sätestatud e-raha ja käesoleva määrusega ettenähtud e-raha tokeni eristamine põhjendatud?<br><br>E-raha direktiivis sätestatu on välja toodud makseasutuste ja e-raha asutuste seaduses, aga see erineb Eestis kehtivast praktikas virtuaalvääringute regulatsiooni osas. See tähendab, et krüptovara on hetkel eristatud e-raha-st nii regulatsiooni, kui kohalduva õiguse ja põhimõtete poolest. Tulenevalt krüptovara erisustest ja selle varasemast praktikas eristamisest, siis ei tuleks e-raha ja e-raha tokeneid ühe mõiste alla liigitada, sest need ei kanna endas sama riski, ohte ning selliselt lõhestatakse krüptovarade regulatsioon, mis võiks olla ühene ja läbiv. Krüptovarade regulatsioon eristamine on muuhulgas vajalik Rahapesu tõkestamise nõukoja (FATF) soovituste ja juhendmaterjalide järgimisel (näiteks riskipõhise lähenemise juhend: http://www.fatfgafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf). Juhul, kui liidu tasemel on ette näha, et krüptovara teenuse pakkujad on tulevikus ühed, ehk tänased krediidi- ja finantseerimisasutused, siis ei pruugi see eristus enam nii oluline olla. Arvestades tegutsevaid krüptovara ettevõtteid ning nende hulka, siis ei ole hetkel seda hinnanguliselt siiski võimalik ette näha. | |
| | 1.4. Kas EL tasemel tuleks üldse reguleerida eraldi kasutustoken'eid, kui jah, siis mis nõuded neile kehtima peaksid?<br><br>Kasutustokenite reguleerimise osas on esialgne seisukoht toodud välja vastusena küsimusele 1.2. Kasutustokenite esmane regulatsioon on vajalik defineerimaks ära eristus teiste tokenite regulatsioonist ning tagamaks, et tulevikus ei võimalda kasutustoken teostada varapõhiste ja e-raha tokenite tegevust, aga ilma igasuguse regulatsioonita.<br>Kasutustokenite osas peaks olema defineeritud nende mõiste, kasutusulatus ning tingimused, millele see peab vastama. Regulatsiooni osas võiks tegemist olla registreerimist vajava tokenite liigiga, et tekitada nende osas usaldusväärsus ning võimalus, et läbi kasutustokenite ei ole võimalik toime panna pettuseid ja/või kelmuseid. | |
| | **2. Küsimused teabe avalikustamise kohta krüptovara emissiooni puhul:**<br>2.1) Kas teie arvates peaks iga krüptovara emissiooni puhul olema nõutud teabedokumendi (st white paper'i) koostamine?<br><br>Teabedokumendi koostamise kohustus iga krüptovara emissiooni osas tekitab suure halduskoormuse järelevalveasutustele. Arvestada tuleb ka asjaoluga, et paljud krüptovarad emiteeritakse tihti ilma igasuguse tulevikus avalduva perspektiivita, seda eriti kasutustokenite teabedokumendi kohustusega reguleerides. Seega peaks teabe-dokumendi kohustus olema krüptovara osas, mida reaalselt praktikas hakatakse kasutama varapõhised ja/või e-raha tokenina, aga siinjuures ei saa kohustuslikuks aluseks olla mõõtmatud alustingimused nagu pakutavate isikute hulk või kaasatav väärtus, sest neid ei ole võimalik liiduüleselt tuvastada ning see muutub liiga kiiresti, et see oleks praktikas tõhusaks meetmeks krüptovara ettevõtete mõistes oluliste arvestuslike alustena. | |
| | 2.2) Kas peaks olema mingi künnis (st pakkumise väärtus, analoogselt väärtpaberite pakkumisega), millest alates pakkumise ja teabedokumendi registreerimine Finantsinspektsioonis oleks emitendile kohustuslik?<br><br>Künnis oma pakkumise ja teabedokumendi registreerimiseks Finantsinspektsioonis peaks praktikas kohustuslik olema. Arvestada tuleb, et krüptovarade puhul peaks pakkumise väärtus olema kindlasti | |

| | | |
|---|---|---|
| | madalam väärtpaberite pakkumisest, sest see sisaldab endas kõrgemaid riske ning ohte. Praktikas on keeruline künnist siduda konkreetse arvuga, sest arvestades hetke turuolukorda oleks kõik mõistlikud künnised halduskoormuse vaates liiga koormavad, aga liiga suure künnise puhul kaotaks see eesmärgi. | |
| | 2.3) Kas Finantsinspektsioon peaks olema teadlik pakkumisest enne selle avalikustamist ning kas Finantsinspektsioonile tuleks esitada teabedokument enne pakkumise avalikustamist?<br><br>Praktikas on krüptovaradele kohalduv regulatsioon ning selle välja kujunemine uudne, mille tõttu paljud teenust pakkuda soovivad isikud ei ole kõikidest neile tulenevatest kohustustest ning täiendavatest nõudmistest teadlik. Seetõttu ei saa usaldada, et tehtav pakkumine on asjakohane ning sobilik, vähemalt mitte eelneva kontrollita. Eeltoodu tõttu ei tohiks pakkumist avaldada enne esmast Finantsinspektsiooni poolset hindamist, aga arutluse alla kuulub küsimus, kui põhjalik see analüüs peab olema, et tagada pakkumiste võimalikus ning nende vastavus regulatsioonidele, aga ka Finantsinspektsiooni teiste seadusest tulenevate ülesannete täitmise jaoks vajalik ressurss. | |
| | 2.4) Mis roll peaks Finantsinspektsioonil olema teabedokumendi saamisel, st kas Finantsinspektsioon peaks kontrollima teabedokumendis esitatud teabe vastavust seaduse nõuetele? Mis peaks olema järelevalve roll emitendi puhul, kes pakub ühekordselt (mitte teenusena) investoritele müügiks krüptovara? Kui Finantsinspektsiooni kontroll on pigem vormiline kui sisuline, siis kas investoril ei või tekkida õiguspärast ootust, et teabedokumendis sisalduv on kontrollitud finantsjärelevalveasutuse poolt?<br><br>Finantsinspektsioonil peab olema teabedokumendi sisulise kontrollimise nõue, sest vastasel juhul puudub neile selle esitamisel eesmärk ning rakendub viidatud õiguspärane ootus, et finantsjärelevalve on teabedokumenti sisuliselt kontrollinud. Vastavat riski ei maanda ka olukord, kus esitatakse teave, et Finantsinspektsioon seda ei kontrolli, sest see ei pruugi kõigi investoriteni jõuda. Emitendi osas, kes pakub teenust ühekordselt võiks kehtida eriregulatsioon, mis tähendab, et ta peaks vastama teatud nõuetele, aga mitte olema võrdsustatud teenuse pakkujatega ning tagatud peab olema, et isik ei saa teenust siiski teatud perioodi jooksul korduvalt pakkuda, näiteks järgneva kolme aasta jooksul. | |
| | **3. Küsimused varapõhiste tokenite ja krüptovara teenuste kohta**<br>3.1) Kas tegevusloa taotlemise künnised varapõhise tokeni emitendile (st emissiooni maht alla 5 mln EUR; pakkumine suunatud kutselistele investoritele; kui emitent on krediidiasutus) on mõistlikud või peaks neid muutma?<br><br>Tegevusloa taotlemise künnis 5 miljonit eurot ei ole kindlasti krüptovarade praeguseid mahte arvestades piisav künnis vaid tegemist peaks olema madalama künnisega. Kutselistele investoritele teenuse pakkumine ei maanda piisavalt riski, et emitent soovib toime panna õigusrikkumise. See küll vähendab riski praktikas realiseerumist, aga see ei peaks olema põhistuseks regulatsiooni alla mitte kuulumisest. | |
| | 3.2) Kui teenuseosutaja korraldab mitu emissiooni, mille maht kokku ületab 5 mln EUR, kas siis emitendile peaks kaasnema tegevusloa kohustus?<br><br>Teenuseosutaja, kes pakub juba ühe emissiooni, mille maht ületab 5 miljonit eurot peaks olema tegevusloa kohustusega ning künnis 5 miljonit eurot peaks olema tunduvalt väiksem, et tagada turu korrastamine. | |
| | 3.3) Kas turu kuritarvitamise regulatsiooni kohaldamine määruse 6. peatükis toodud ulatuses (sh siseteabe avaldamise-, siseteabe alusel | |

| | | |
|---|---|---|
| | kauplemise ning turumanipulatsiooni keeld) on teie arvates piisav, vajalik ja põhjendatud?<br><br>Ainuüksi nõuete määrusesse sätestamine ei ole piisav, et tagada turu kuritarvitamise tõkestamine. Arvestades sektori võrreldavust krediidiasutuste ja finantseerimisasutustega ning asjaoluga, et krüptovarade ja nendega seonduvaid teenuseid pakkuvad ettevõtted on nii killustatud ning hetkel ilma sisuliste nõueteta, siis vaid vormiliste rikkumise nõuete sätestamine tekitab kindlasti muudatuste ülevõtmisel ning järgneval perioodil palju rikkumisi, sest kehtivad vaid üldised piirangud ning kuigi on olemas isikute sobivuse nõuded ja sektorisse sobivuse nõuded, siis sektori sobivuse nõuetele vastavad hetkel praktikas teenust pakkunud isikud, kelle osas ei ole sobivusnõuete osas võibolla veel asjakohast hinnangut, sest varasemalt on sektor alareguleeritud olnud. Lisaks ei vähendata riski, et kasutatakse peidetud tegelikke kasusaajaid ning teiste isikute juhtimist, mille kaudu jäävad varju ebakorrektse ärialase mainega isikud. See tähendab, et nõuete sätestamine ei taga nende järgimist ning turu alaregulatsiooni tõttu on algselt palju rikkumisi, mistõttu peaks turu kuritarvitamise regulatsiooni meetodid olema tagatud organisatoorsete põhjalike järelevalveliste, audiitorikohustuse ning infoturbe ja andmekaitsealaste nõuetega, mille osas on iseregulatsioon ning täiendav järelevalve funktsioon. Kindlasti on tegemist vajalike ja põhjendatud nõuetega, aga need peavad toimima koosmõjus kogu krüptovarade sektori regulatsiooniga. | |
| | 3.4) Kas krüptovara teenuse pakkujal peaks olema lubatud enda poolt hallataval platvormil oma arvel krüptovaradega kaubelda?<br><br>Selliselt teenuse pakkumine tekitab väga suure turu manipulatsiooni ning ärakasutamise ohu, mis arvestades hetke regulatsioone ei saa olla piisav tagamaks tarbijate ning klientide õiguste ja varade kaitse. Eeltoodud tõttu ei tohiks vastav tegevus lubatud olla või vähemalt ei tohiks see lubatud olla enne, kui vastavad riskid on praktikas päriselt maandatud. | |
| | 3.5) Kas teie arvates on krüptovara kauplemisplatvormile sätestatud nõudeid praktikas võimalik efektiivselt täita?<br><br>Krüptovara kauplemisplatvormidele määruses toodud nõudeid, mis omavad organisatoorset olemust on võimalik praktikas täita. Küsitav on vastava teabe jagamisest ja kättesaadavusest seda nii pädevate järelevalveasutuste vahel, aga ka teiste asutustega. Arvestades kõiki nõudeid, siis kindlasti ei suuda neid kohustusi ja nõudeid täita kõik hetkel Euroopa Liidus teenust pakkuvad krüptovara kauplemisplatvormid, mis tekitab küsimuse üleminekuperioodist ning nende nõuete kontrollimisest ja vastavuse hindamisest. Arvestades, et tegemist on teatud ulatuses kaalutlust omavate nõuetega erineb kindlasti riikidevaheline praktika selles küsimuses, mille tõttu on keeruline tagada, et kõik riigid kohaldavad määrust ühetaoliselt, mis võib anda ebaõige konkurentsieelise leebemalt tõlgendavatele liikmesriikidele. Keeruline on tagada, et artiklis 59 toodud nõuded oleks igal hetkel tagatud, sest teada ei ole selliste teenuse pakkujate arv ning järelevalve teostamise võimalikkus. Täiendavalt tuleb analüüsida, et kuidas täpselt reguleeritakse teenuse pakkumise kohta, sest Euroopa Liidu Kohtu praktika ei anna selles küsimuses ammendavat seisukohta, aga krüptovarade puhul on tegemist veebipõhiselt pakutava teenusega, mida kindlasti üritatakse nõuete karmistumisel pakkuda kolmandatest riikidest Euroopa Liidu kodanikele, mistõttu tuleks tagada ka nõuete kohaldumise juba Euroopa Liidu kodanikule teenuse pakkumisel. | |
| | **4. Muud tähelepanekud ja kommentaarid (vabas vormis):** | |

| | | |
|---|---|---|
| | Määruse osas ei ole arvestatud kehtivate regulatsioonidega ning see ei lähe otseselt kooskõlla Eesti praktikaga. Eestis kehtib virtuaalvääringute regulatsioon juba 2017. aasta lõpust, mis on oluliselt varasem, kui vastav kohustus EL direktiiviga 2018/843 praktikasse tegelikult tekkis. See tähendab, et Eestis on juba väljakujunenud praktika virtuaalvääringu teenuse pakkumise tegevusloa regulatsiooni osas ning turuosalistel on teatud õigustatud ootus kohalduva regulatsiooni osas. Määruses välja pakutu puhul on pigem tegemist Finantsinspektsiooni järelevalve alla kuuluva teenusega (mida kinnitab ka käesolev küsimustik), aga hetkel on virtuaalvääringute järelevalve rahapesu andmebüroo all. See tähendab, et määrusega vastavuses olemiseks tuleks Eestis ümber korraldada virtuaalvääringute teenuse pakkujate järelevalve.<br>Määrus sätestab teatud juhtudel leebemad nõuded, kui seda teeb kehtiv regulatsioon, näiteks menetlustähtajad, mis praktikas on maksimaalselt 120 päeva, aga määruse tekstis maksimaalselt 25 tööpäeva. Arvestades virtuaalvääringute tegevuslubade arvu hetkel (üle 200) ei ole praktikas reaalne järgida kõiki määruses toodud nõudeid, sest järelevalveasutusel ei ole selle ajakulu täitmiseks piisavalt ressurssi (nii hetkel rahapesu andmebüroo, kui võimalik tulevikus Finantsinspektsioon). Lisaks ei puuduta määrus peamiseid rahapesu ja terrorismi rahastamise tõkestamise kohustusi ja nõudeid, mida kehtiv regulatsioon teeb. Lisaks käsitleb määrus omanike kontrolli kohustust vaid teatud protsendist alates, kehtiv regulatsioon algab sõltumata protsendist vaid piisab omandist kui faktist.<br>Määruse osas tuleks hinnata, kas selles sätestatu on liiga põhjalik, kui soovitakse maandada vaid otsest krüptovaradest tuleneva kahjuliku mõju tagajärgi või kas tegemist on liiga leebe regulatsiooniga, kui soovitakse reguleerida krüptovaradest tulenevaid riske ning ohte, millisel juhul tagatakse ka ennetav funktsioon. Hetkel ei ole lahendus siiski piisav, et tagada krüptovaradest tulenev riskide ja ohtude maandamine ning vaid teatud künnisest, mis on Eesti vaatest üsna kõrge, ülespoole jäävate teenuste reguleerimine tekitab küsimuse künnise alla jäävatest teenustest, nende järelevalvest ning finantssektori ühetaolisest järelevalvest. | |
| | | |
| **7** | **Tarbijakaitse ja Tehnilise Järelevalve Amet** | |
| | Arvamuse esitamine finantsteenuste digitaalse operatsioonilise resilientsuse akti (DORA) kohta<br>Täname Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu (edaspidi ITL) kaasamise eest finantsteenuste digitaalse operatsioonilise resilientsuse (DORA) konsultatsiooni.<br>Arvestades materjali mahukust ja tagasiside andmise lühikest perioodi, jõudsime me analüüsida ainult ettepanekut kehtestada järelevalveraamistik teenusepakkujatele (näiteks kõrgtehnoloogia ettevõtjad ehk Big Techs), kes pakuvad finantsasutustele pilvandmetöötlust või mõnda muud olulist teenust. Seoses sellega teeme ettepaneku jätta info- ja kommunikatsiooni teenuse pakkujatele mõeldud reeglid määrusest välja, et vältida järjekordsete sektorspetsiifiliste reeglite teket. | |
| | **Tagasiside krüptovarade määruse kohta** | |
| | **<u>1. Tagasiside krüptovarade määruse kohaldumisala kohta</u>**<br><u>1.1. Kas teie arvates on määruse eelnõu (edaspidi määrus) kohaldamisalasse jäävad instrumendid ja nende liigitus (kõikvõimalikud token'id, sh kasutustoken'id (utility tokens) ja varapõhised tokenid (asset-referenced token) ja e-raha tokenid) põhjendatud?</u> | |

| | | |
|---|---|---|
| | Kuigi esmapilgul võib tunduda, et kasutustokenite reguleerimine kavandatavas määruses ei pruugi olla asjakohane, sest kasutustokenite puhul puudub võimalus teenida finantstulu ning sellest lähtuvalt on ka nimetatud krüptovaradega väiksemad riskid, siis on TTJA hinnangul, et tokenite sellisel kujul liigitamine määruse eelnõus on põhjendatud. Seda lähtuvalt just tarbijate kaitsmise vajadusest. Ka täna on TTJA puutunud kokku tarbijate kaebustega, kus neile on jäänud arusaamatuks, et miks nende soetatud krüptovarad (kasutustoken) ei ole kaubeldavad ning on ainult kasutatavad üksikutes kohtades, muutes nende nn investeeringu sisuliselt mõttetuks. Kuigi tarbijate kaebuste arv seoses just kasutustokenitega on suhteliselt vähene (üksikud kaasused), siis on näha, et erinevad kelmused erinevate krüptovaradega on kasvavas trendis.<br><br>Samuti katab praegusel kujul määruse kohaldamisalasse jäävate instrumentide liigitus sisuliselt kogu krüptovarade spektri, mille läbi saavutatakse suurem õiguskindlus ja õigusselgus ning tulenevalt sellest ka parem tarbijate kaitse. | |
| | 1.2. Kas määruse kohaldamisala tuleks siiski muuta/piiritleda ja määratleda määruse kohaldumisalasse kuuluva krüptovara vormi nii, et see oleks seotud eelkõige finantstulu teenimisega ja/või investeerimisriskiga?<br><br>Ei (vt vastust küsimusele 1.1). | |
| | 1.3. Kas teie arvates on e-raha direktiivis sätestatud e-raha ja käesoleva määrusega ettenähtud e-raha tokeni eristamine põhjendatud?<br><br>Sellisel kujul eristamine on TTJA hinnangul põhjendatud, sest mõisted sisaldavad olulisi erinevusi. Nimetatud asjaolule viidatakse ka määruse preambuli punktis 10. | |
| | 1.4. Kas EL tasemel tuleks üldse reguleerida eraldi kasutustoken'eid, kui jah, siis mis nõuded neile kehtima peaksid?<br><br>Eraldi regulatsioon ei ole vajalik, kui reguleeritakse kavandatavas määruses. Kui kasutustoken'eid peaksid kõnes olevast määrusest siiski välja jääma, siis eraldi regulatsioon EL-i tasandil ei ole mõistlik. Sellisel juhul tuleks lähtuda siseriiklikest regulatsioonidest. | |
| | **2. Küsimused teabe avalikustamise kohta krüptovara emissiooni puhul:**<br>2.1. Kas teie arvates peaks iga krüptovara emissiooni puhul olema nõutud teabedokumendi (st white paper'i) koostamine?<br><br>Tarbijate informeerimise huvides peaks krüptovarade emissiooni puhul olema nõutud teabedokumendi koostamine. | |
| | 2.2. Kas peaks olema mingi künnis (st pakkumise väärtus, analoogselt väärtpaberite pakkumisega), millest alates pakkumise ja teabedokumendi registreerimine Finantsinspektsioonis oleks emitendile kohustuslik?<br><br>Eraldi künnise seadmine ei ole vajalik, kui kehtib üleüldine teabedokumendi esitamise kohustus. Erisused on kavandatava määruse tekstis ka välja toodud, millal ei pea teabedokumenti esitama. | |
| | 2.3. Kas Finantsinspektsioon peaks olema teadlik pakkumisest enne selle avalikustamist ning kas Finantsinspektsioonile tuleks esitada teabedokument enne pakkumise avalikustamist? | |

| | | |
|---|---|---|
| | Kindlasti tuleks Finantsinspektsiooni informeerida pakkumisest ning teabedokumendid esitada enne pakkumise avalikustamist. Vastasel juhul ei täidaks teavitus või teabedokumendi esitamine oma eesmärki. Samuti on Finantsinspektsioonil võimalus vajadusel juba enne pakkumis sekkuda. | |
| | 2.4. Mis roll peaks Finantsinspektsioonil olema teabedokumendi saamisel, st kas Finantsinspektsioon peaks kontrollima teabedokumendis esitatud teabe vastavust seaduse nõuetele? Mis peaks olema järelevalve roll emitendi puhul, kes pakub ühekordselt (mitte teenusena) investoritele müügiks krüptovara? Kui Finantsinspektsiooni kontroll on pigem vormiline kui sisuline, siis kas investoril ei või tekkida õiguspärast ootust, et teabedokumendis sisalduv on kontrollitud finantsjärelevalveasutuse poolt?<br><br>Kuna *ex ante* kooskõlastus teabedokumendile ei ole määruse teksti kohaselt nõutav, siis täidab Finantsinspektsioon turujärelevalve funktsioone ning teostab teabedokumendi kontrolle vastavalt vajadusele (nt risikanalüüsi põhiselt vms). Ainuüksi teabedokumendi esitamise nõue peaks krüptovaluuta pakkujate turgu juba iseenesest korrastama.<br><br>Lähtuda tuleks antud juhul hea usu põhimõttest, et esitatud dokumendid on korrektsed ning ei sisalda valeandmeid. Samas on näiteks Eestis olemas ka karistusõiguslikud meetmed haldusorganile teadvalt valeandmete esitamise osas. Seega peaks sellised meetmed olema juba piisava heidutusega, tagamaks et esitatakse korrektseid andmeid. | |
| | **3. Küsimused varapõhiste tokenite ja krüptovara teenuste kohta**<br>3.1. Kas tegevusloa taotlemise künnised varapõhise tokeni emitendile (st emissiooni maht alla 5 mln EUR; pakkumine suunatud kutselistele investoritele; kui emitent on krediidiasutus) on mõistlikud või peaks neid muutma?<br><br>Kuna sellistel emitentidel on jätkuvalt teabedokumentide esitamise kohustus tururegulaatorile, siis halduskoormuse vähendamise ning ressursside piiratud mahu tingimustes on sellise künnise seadmine mõistlik. Vajadusel saab näiteks Finantsinspektsioon jätkuvalt sekkuda. | |
| | 3.2. Kui teenuseosutaja korraldab mitu emissiooni, mille maht kokku ületab 5 mln EUR, kas siis emitendile peaks kaasnema tegevusloa kohustus?<br><br>Kui teenuseosutaja korraldab mitu emissiooni, mille maht kokku ületab 5 mln EUR, siis sellega peaks kaasnema ka tegevusloa kohustus. Vastasel juhul hakatakse nn auku kindlasti ka ära kasutama ning teenuseosutajad, kellel muidu peaks olema tegevusloa kohustus saaksid nimetaud loakohustust vältida sellega, et emissioone hakatakse hajutama. | |
| | 3.3. Kas turu kuritarvitamise regulatsiooni kohaldamine määruse 6. peatükis toodud ulatuses (sh siseteabe avaldamise-, siseteabe alusel kauplemise ning turumanipulatsiooni keeld) on teie arvates piisav, vajalik ja põhjendatud?<br><br>TTJA ei ole pädev nimetaud küsimusele vastama. Seisukoht puudub. | |
| | 3.4. Kas krüptovara teenuse pakkujal peaks olema lubatud enda poolt hallataval platvormil oma arvel krüptovaradega kaubelda?<br><br>Võimalike huvide konflikti vältimiseks ei tohiks olla lubatud teenusepakkujal enda poolt hallataval platvormil oma arvel krüptovaradega kaubelda. | |
| | 3.5. Kas teie arvates on krüptovara kauplemisplatvormile sätestatud nõudeid praktikas võimalik efektiivselt täita? | |

| | | |
|---|---|---|
| | TTJA ei ole pädev nimetaud küsimusele vastama. Seisukoht puudub. | |