17.11.2020

SELETUSKIRI

EESTI SEISUKOHAD EUROOPA KOMISJONI 2020. AASTA SEPTEMBRI TEGEVUSKAVADE JA ALGATUSTE KOHTA

SISUKORD

1 SISSEJUHATUS

1.1. Digirahanduse paketi ettepanekud ja teatised

Euroopa Komisjon (edaspidi *komisjon*) avaldas 2020. a 24. septembris ELi digirahanduse strateegia, ELi jaemaksete strateegia ja seotud õigusaktide paketi (edaspidi ***digirahanduse pakett***), mis koosneb järgmistest teatistest ja algatustest:

1) Komisjoni teatis KOM(2020) 591 Euroopa Parlamendile, nõukogule, Euroopa majandus- ja sotsiaalkomiteele ning regioonide komiteele EL-i digirahanduse strateegia kohta[1];
2) Komisjoni teatis KOM(2020) 592 Euroopa Parlamendile, nõukogule, Euroopa majandus- ja sotsiaalkomiteele ning regioonide komiteele EL-i jaemaksete strateegia kohta[2];
3) Euroopa Parlamendi ja nõukogu määruse ettepanek KOM(2020) 593 krüptovaraturgude kohta ja millega muudetakse direktiivi (EL) 2019/1937;
4) Euroopa Parlamendi ja nõukogu määruse ettepanek KOM(2020) 594 hajutusraamatu tehnoloogial põhinevate turuinfrastruktuuride katserežiimi kohta;
5) Euroopa Parlamendi ja nõukogu määruse ettepanek KOM(2020) 595 finantsteenuste digitaalse operatsioonilise resilientsuse kohta ja millega muudetakse määrusi (EL) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014 ja (EL) nt 909/2014;
6) Euroopa Parlamendi ja nõukogu direktiivi ettepanek KOM(2020) 596, millega muudetakse direktiive 2006/43/EÜ, 2009/65/EÜ, 2009/138/EÜ, 2011/61/EL, EU/2013/36, 2014/65/EL, (EL) 2015/2366 and EL/2016/2341**.**

Seega digirahanduse paketi raames algatatakse kolm uut määrust ja üks direktiiv. Kõigi määruste ettepanekute õiguslik alus on Euroopa Liidu toimimise lepingu artikkel 114. Direktiivi ettepaneku õiguslik alus on Euroopa Liidu toimimise lepingu artikli 53 lõige 1 ja artikkel 114. Õigusaktide vastusvõtmiseks on nõukogus vaja kvalifitseeritud häälteenamust. Ettepanekute subsidiaarsustähtaeg on […][3]. Krüptovaraturgude ettepanekute subsidiaarsustähtaeg on 29. jaanuar 2021.

Hetkeseisuga on Saksamaa eesistumisel toimunud ka esimesed nõukogu töögruppide kohtumised - krüptovääringute regulatsiooni osas 29. septembril, 29. oktoobril ja 13. novembril, finantsteenuste operatsioonilise vastupidavusega seotud regulatsiooni osas 30. septembril, 22. ja 28. oktoobril ning 9. novembril. Kuna tegemist on mahuka ettepanekute paketiga, on arutelud alles algusjärgus. Kapitaliturgude liidu tegevuskava ja digirahanduse paketti arutati ka ECOFINi 6. oktoobri 2020. a kohtumisel. Ministrite arutelu kokkuvõttes sai nõukogu töögrupp mandaadi alustada tööd paketiga. Eesmärkideks i) vähendada fragmenteeritust digitaalsel siseturul, (ii) kohandada EL õigus digiajastule vastavaks ja (iii) tõhustada andmete efektiivsemat kasutamist konkurentsieeliste loomiseks.

1.2. Digirahanduse paketist üldisemalt

Euroopa Komisjon võttis 24. septembril vastu ELi digirahanduse ja ELi jaemaksete strateegiate ning seotud õigusaktide paketi, mis tugineb 2018. aasta finantstehnoloogia tegevuskava raames ja 2020. aasta kevadel toimunud konsultatsioonide raames tehtud tööle.

Pakett toetab majanduse taaskäivitamist, Euroopa rohelise kokkuleppe ja Euroopa uue tööstusstrateegia elluviimist. Paketi mõjul soovitakse finantssektori reeglid muuta digisõbralikumaks ning tugevdada tarbijate turvalisust ja vastutustundlikku innovatsiooni finantssektoris (eelkõige väga uuenduslike digitaalsete idufirmade puhul, leevendades samal ajal võimalikke investorite kaitse, rahapesu ja küberkuritegevusega seotud riske).

[1] Eesti keeles: https://eur-lex.europa.eu/legal-content/ET/TXT/?qid=1601982766470&uri=CELEX:52020DC0591
[2] Eesti keeles: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52020DC0592&qid=1601983025032
[3] Läbirääkimised EL nõukogu tasandil on alanud. Õigusaktide ettepanekute tõlkeid veel ei ole ja seega subsidiaarsustähtaega ei ole veel määratud

Digirahanduse strateegia mõjul peaks väiksemate riskidega uuenduslike finantstoodete kättesaadavus tarbijatele ja ettevõtete ligipääs rahastamisvõimalustele veelgi paranema. Pakett toetab ka turvalisi lahendusi tehisintellekti, plokiahela ja andmehalduse kasutamiseks.

Jaemaksete strateegia eesmärk on Euroopas turvaliste, kiirete ja usaldusväärsete makseteenuste pakkumine. Strateegia keskendub ELis täielikult integreeritud jaemakse keskkonna väljaarendamisele, sealhulgas üleminekut välkmaksetele ning avatud panganduse põhimõtte rakendamisele. Strateegia raames on kavandatud makseteenuste direktiivi ülevaatamine ja vajadusel selle ajakohastamine 2021. aasta neljandas kvartalis.

Finantsteenuste digitaalse operatsioonilise resilientsuse õigusakti peamiseks eesmärgiks on ennetada ja maandada finantssektoris esinevaid digitaalseid riske, sh küberriske. Euroopa Komisjoni hinnangul tähendab finantssektori järjest suurem sõltuvus tarkvarast ja digitaalsetest protsessidest ka info- ja kommunikatsioonitehnoloogiaga (IKT) seotud riskide tõusu. Seetõttu teeb komisjon suurele hulgale finantsteenuste ettevõtjatele ettepaneku tagada, et nad suudaksid vastu pidada igat tüüpi IKT-ga seotud häiretele ja ohtudele. Pangad, börsid, arvelduskojad ja ka finantstehnoloogia ettevõtjad peavad IKT-ga seotud juhtumite ennetamiseks ja riskide maandamiseks järgima seega rangeid standardeid.

Määrus hõlmab järgmisi valdkondi:

- IKT riskijuhtimine;
- suurtest IKT intsidentidest raporteerimine pädevale asutusele;
- digitaalse operatsioonilise resilientsuse testimine;
- küberohtudega ja haavatavustega seotud infojagamine;
- kolmandatest osapooltest IKT teenuseosutajatega seotud riskide juhtimise ja maandamise meetmed;
- finantsteenuse osutaja ja kolmandast osapoolest IKT teenuseosutaja vahelistele lepingutele kohalduvad printsiibid;
- kolmandatest osapooltest IKT teenuseosutajate järelevaatamise raamistik;
- pädevate asutuste koostöö ja järelevalve.

Krüptovaraturgude õigusakti peamiseks eesmärgiks on kehtestada EL määrus krüptovarade reguleerimiseks. Nimetatud määruse kohaldumisalasse kuuluksid kõik krüptovarad, mis ei ole finantsinstrumendid või investeerimishoius MiFID II tähenduses, e-raha EMD2 tähenduses, hoius hoiuste tagamise skeemide direktiivi tähenduses või väärtpaberistamine väärtpaberistamise direktiivi tähenduses, ja nn "*stablecoin*"-id, ning nimetatud krüptovarade emiteerimise ja käitlemisega seotud teenuseosutajad. Mis puudutab konkreetseid nõudeid, siis krüptovara emitentidele olulisi muudatusi ei kaasne – kohustuslikuks tehakse põhiteabedokumendi, mille sisu peab vastama määruse nõuetele, avalikustamine, aga järelevalveasutused ei kontrolliks selle sisu. Kõige rangemalt on reguleeritud e-raha tokenid ja varapõhised tokenid (*asset-referenced tokens*), mille puhul peab emitent taotlema tegevusloa ning saama oma instrumendi põhiteabedokumendi sisule eelneva heakskiidu.

Hajutusraamatu tehnoloogial põhinevate turuinfrastruktuuride katserežiimi eesmärgiks on edendada krüptograafilisel kujul esitatud MiFID väärtpaberite arendamist ja kasutuselevõttu ning anda võimalus tutvuda sellisel kujul esitatud väärtpaberite käibega. Pilootrežiim annab võimaluse hajusraamatu infrastruktuuridel (mitmepoolne kauplemiskoht MIFID 2 mõistes ja väärtpaberiarveldussüsteem CSDR mõistes) taotleda MiFID II ja CSDR-ist tulenevate nõuete mitte-kohaldamist.

1.3. Siseriikliku õiguse muutmise vajadus

Siseriiklikult võib osutada vajalikuks muuta finantsinspektsiooni seadust, küberturvalisuse seadust, audiitortegevuse seadust, kindlustustegevuse seadust, väärtpaberituru seadust, makseasutuste ja e-raha asutuste

seadust, investeerimisfondide seadust ja krediidiasutuste seadust (eelkõige tulenevalt direktiivi[4] siseriiklikku õigusesse ülevõtmisest).

Krüptovarade ettepanekuga seotud muudatused viiakse tulevikus sisse käesoleval ajal kavandatavasse ühisrahastuse ja muude investeerimisinstrumentide ning virtuaalvääringute seadusesse (ÜMIVS), mille eelnõu esimene konsultatsioon toimub käesoleva aasta lõpus. Finantsteenuste digitaalse operatsioonilise vastupidavuse ettepanekuga seotud muudatuste tegemise vajadus riigisiseses õiguses võib puudutada eeskätt küberturvalisuse seadust ja finantsinspektsiooni seadust.

1.4. Huvirühmade kaasamine

Rahandusministeerium on seisukohtade ettevalmistamisel pöördunud arvamuse saamiseks Justiitsministeeriumi, Majandus- ja Kommunikatsiooniministeeriumi, Siseministeeriumi, Finantsinspektsiooni, Eesti Panga, Politsei- ja Piirivalveameti, Rahapesu Andmebüroo, Finance Estonia MTÜ, Eesti Pangaliidu, Nasdaq Tallinna Börsi, Eesti Infosüsteemise Ameti, Eesti Kindlustusseltside Liidu, Eesti Kindlustusmaaklerite Liidu, investeerimisühingute, Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu, Eesti Advokatuuri, Eesti Krüptoraha Liidu, Audiitorkogu poole ning Tarbijakaitse ja Tehnilise Järelevalve Ameti poole.

Arvamuse andsid Majandus- ja Kommunikatsiooniministeerium koos RIAga, Siseministeerium koos allasutustega, Finantsinspektsioon, Eesti Pank, Eesti Pangaliit, Eesti Infotehnoloogia ja Telekommunikatsiooni Liit, Rahapesu Andmebüroo ning Tarbijakaitse ja Tehnilise Järelevalve Amet. Esitatud arvamustega on Eesti seisukohtade kujundamisel võimaluse korral arvestatud.

1.5. Eelnõu ettevalmistajad

Eelnõu ja seletuskirja on koostanud Rahandusministeeriumi finantsturgude poliitika osakonna jurist Paula Etti (+372 611 3502, paula.etti@fin.ee), sama osakonna peaspetsialist Kristen Leppik (6113093, Kristen.leppik@fin.ee), kindlustuspoliitika osakonna jurist Linda Lelumees (6113550, linda.lelumees@fin.ee) ja sama osakonna peaspetsialist Kristiina Kubja (6113658, kristiina.kubja@fin.ee).

2 DIGIRAHANDUSE PAEKTT

2.1 DIGIRAHANDUSE STRATEEGIA

Digirahanduse strateegias on kindlaks määratud Euroopa digirahanduse peamised prioriteedid ja eesmärgid järgmiseks neljaks aastaks. Nende eesmärkide saavutamiseks võtab komisjon mitmeid olulisi meetmeid.

Strateegiline eesmärk: kasutada ära digirahanduse võimalusi tarbijate ja ettevõtjate hüvanguks.

Prioriteedid:

1) kõrvaldada finantsteenuste digitaalse ühtse turu killustatus, võimaldades seeläbi Euroopa tarbijatele juurdepääsu piiriülestele teenustele ja aidates Euroopa finantsettevõtetel laiendada oma digitaalset tegevust;
2) tagada, et ELi õigusraamistik hõlbustaks digitaalset innovatsiooni tarbijate ja turu tõhususe huvides;
3) luua Euroopa finantsandmete ruum, et edendada andmepõhist innovatsiooni, tuginedes Euroopa andmestrateegiale, sealhulgas laiendada juurdepääsu andmetele ja andmete jagamist finantssektoris;
4) tegeleda digiüleminekuga seotud uute väljakutsete ja riskidega.

[4] COM(2020) 596, 2020/0268(COD). Viidatud direktiivi ettepanekuga soovitakse muuta järgmisi direktiive: 2006/43/EC (raamatupidamise aruanded), 2009/65/EC (UCITS, eurofondid), 2009/138/EU (Solvency II, edasikindlustus), 2011/61/EU (AIFMD, alternatiivsed investeerimisfondid), EU/2013/36 (CRD, kapitalinõuded), 2014/65/EU (MIFID2, finantsinstrumendid), (EU) 2015/2366 (PSD2, makseteenused) and EU/2016/2341 (IORPs, tööandjapension).

Peamised meetmed:

1) 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 koostalitlusvõime piiriülest raamistikku (prioriteet 1).
2) Komisjon uurib vajadust kehtestada täiendav ühtlustatud litsentsimis- ja tegevusloa andmise kord, teeb Euroopa innovatsioonisoodustajate foorumi (EFIF)[5] tugevdamiseks koostööd Euroopa järelevalveasutustega ja loob ELi digirahanduse platvormi[6], et edendada koostööd era- ja avaliku sektori sidusrühmade vahel (prioriteet 1).
3) Komisjoni ettepanek uue ELi õigusraamistiku kohta, mis käsitleb krüptovara, sealhulgas varapõhiseid tokeneid (nn stabiilne krüptovara (stablecoins)) ja kasutustokeneid (prioriteet 2).
4) Komisjon tagab korrapäraste läbivaatamiste abil, et kõrvaldatakse innovatsiooni pärssivad võimalikud olulised regulatiivsed tõkked, mis tulenevad finantsteenuseid käsitlevatest õigusaktidest. Komisjon annab korrapäraselt tõlgendamissuuniseid selle kohta, kuidas kohaldada finantsteenuseid käsitlevaid kehtivaid õigusakte uute tehnoloogiate suhtes (prioriteet 2).
5) Komisjon muudab ELi õigusakte, et tagada avalikustatud teabe kättesaadavus standardses ja masinloetavas vormingus, ning loob avalikustamiseks ELi rahastatava taristu (prioriteet 3).
6) Komisjon esitab 2021. aastal järelevalveandmete strateegia (prioriteet 3).
7) Komisjon esitab 2022. aasta keskpaigaks seadusandliku ettepaneku uue avatud rahanduse raamistiku kohta, tuginedes andmetele juurdepääsu laiematele algatustele ja nendega täielikus kooskõlas (prioriteet 3).
8) Komisjon teeb 2022. aasta keskpaigaks ettepaneku teha kehtivas finantsteenuste õigusraamistikus vajalikud kohandused seoses tarbijakaitse ja usaldatavusnõuetega, et kaitsta digirahanduse lõppkasutajaid, tagada finantsstabiilsus, kaitsta ELi finantssektori usaldusväärsust ja tagada võrdsed tingimused (prioriteet 4).
9) Komisjon esitab täna ettepaneku uue ELi raamistiku kohta, mille eesmärk on tugevdada digitaalset operatsioonilist vastupidavusvõimet ehk tegevuskerksust (prioriteet 4).

Mõju Eestile. *Kavandatavad muudatused mõjutavad Eestist positiivselt, kuna kõnealuse strateegia meetmed võimaldavad vähendada digitaalse ühtse turu killustatust, et ka Eesti tarbijatel oleks piiriüleselt parem juurdepääs finantstoodetele ning et finantstehnoloogia idufirmad saaksid oma tegevust laiendada ja kasvada. Majandus- ja Kommunikatsiooniministeeriumi hinnangul tunduvad strateegias välja toodud ideed toetavat ka meie fintech startupide tegevusi. Saame üldjuhul toetada Euroopa üleselt seatud eesmärke ja oleme valmis neid rakendama, kuid saame täpsemalt mõjusid hinnata juba konkreetsete regulatiivsete ettepanekute põhjal.*

2.2 JAEMAKSETE STRATEEGIA

Kommunikatsioonidokument jaemaksete strateegia kohta (communication on Retail Payments strategy for the EU) on aluseks edaspidi maksekeskkonna kujundamisel ja sellest lähtutakse makseteenuseid ja maksekeskkonda puudutavate algatuste – ELi õigusaktide väljatöötamisel. Selle strateegia keskendub neljale põhiteemale:

- **Euroopaülesed välkmaksed kui uus normaalsus**
- **Innovaatiline ja konkurentsivõimeline maksekeskkond**
- **Tõhusam ja koostalitusvõimelisem maksetaristu**
- **Tõhusamalt toimivad rahvusvahelised maksed**

[5] EFIF loodi pärast Euroopa järelevalveasutuste 2019. aasta jaanuari ühisaruannet regulatiivsete katsetuskeskkondade ja innovatsioonikeskuste kohta, milles toodi esile vajadus meetmete järele, millega edendada innovatsioonisoodustajate vahelist koordineerimist ja koostööd, et toetada finantstehnoloogia laiemat kasutuselevõttu ühtsel turul, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2020:0591:FIN:ET:PDF, lk 8.

[6] Era- ja avaliku sektori sidusrühmade koostöö soodustamiseks loob komisjon koostöös EFIFiga uue ELi digirahanduse platvormi. Uus platvorm toimib uue digirahanduse ökosüsteemiga internetis pideva suhtlemise kanalina, tuginedes digirahanduse valdkonna teabevahetuse raames saadud positiivsele tagasisidele. Samuti annab see liidese EFIFile ning riiklikele innovatsioonisoodustajatele ja riiklikele e-litsentside andmise menetlustele. Edaspidi võib selle kujundada laiemaks koostööplatvormiks ja andmeruumiks, mida sektor või järelevalveasutused saavad kasutada innovaatiliste lahenduste katsetamiseks. Platvorm töötatakse välja nii, et seda oleks võimalik rahastada programmist „Digitaalne Euroopa“, mis toetab digitehnoloogia süvalaiendamise koostööplatvormide kasutuselevõttu. Allikas: ibid.

Välkmaksed kui uus normaalsus: Uute makse algatamise võimaluste otsimisega tegeletakse pidevalt. Turule on tulnud nii uusi makseinstrumente (nutikell, mobiil jm seade), kui ka välja töötatud täiesti instrumendivabu makse algatamise võimalusi (nt erinevad näo või sõrmejälje tuvastustehnoloogiad).

Erinevate makselahenduste puudusena tuuakse välja, et neil puudub Euroopaülene kasutusvõimalus. Kreeditkorraldusel põhineva välkmakse juurutamine on midagi, mis võiks seda eesmärki täita – see oleks kasutusel ja toimiks ühtsetel alustel ELi üleselt, pakuks konkurentsi teistele makse algatamise lahendustele, sh kaardimaksesüsteemile, mis omakorda aitaks suurendada ka sõltumatust teistest makselahendustest.

Tulevikunägemuses oleks välkmaksete täielik kasutusele võtmine 2021 a lõpuks.

Ühes välkmaksete propageerimisega tegeletakse samaaegselt makseteenuste kasutajale suunatud lahenduste väljatöötamisega, et teha makse algatamine teenuse klientidele võimalikult mugavaks ja mis toimiksid maksekaardi asemel, nt mobiiltelefoni maksed.

Muudatusettepanekute eeltööna näeb strateegidokument ette, et seoses välkmaksete juurutamisega tuleb tegeleda pankade likviidsusküsimustega seoses välkmaksetega väljaspool pangapäeva, hinnata välkmaksetega seotud rahapesu riske, digitaalsete autentimisvõimaluste kasutamist erinevate riikides, viipemakse võimekusega riigiasutustes, haiglates jm.

Strateegiadokumendi kohaselt tuleb Komisjon välja ettepanekutega, mis kohustavad teatud makseteenuse pakkujaid pakkuma välkmakseid ja liituma selleks loodud süsteemiga 2021 aasta lõpuks.

Innovaatiline ja konkurentsivõimeline jaemaksete keskkond. Sellel tegevussuunal on märksõnaks avatud pangandus. Siin on kavas makseteenuste teise direktiivi ülevaatamine, rakendamise mõjuhinnangu läbiviimine ja selle pinnalt uute ettepanekute tegemine. Eesmärgiks on turvalisuse tõstmine (näiteks muuta kohustuslikuks makse saaja ja kontotunnuse (IBANi) kontrollimine või milliselt domeeniaadressilt sooritatakse autentimine), turuosaliste võrdse kohtlemise ja tarbijamugavuse tagamine. Näiteks, uuritakse võimalusi viipemaksete määra tõstmiseks, samuti seda, kas olemasolev makseteenuste regulatsioon tekitab turul ebavõrdset konkurentsi või toob kaasa suurenenud riske (nt infotehnoloogiliste teenuste raames).

Ühtlasi selgitatakse välja, kas e-raha teenuse pakkujate suhtes eraldi regulatsiooni hoidmine on edaspidi õigustatud. Strateegia kohaselt on oodata makseteenuste valdkonna muudatusettepanekuid aastal 2022.

Tõhusam ja koostalitlusvõimelisem maksetaristu. Mitmes lepinguriigis on välkmaksed riigisiseselt kasutusel, kuid see ei ole tagatud piiriüleselt. Välkmaksete toimimine piiriüleselt saab olla tagatud juhul, kui arveldamist võimaldavad süsteemid on omavahel ühendatud. Erinevate jaemaksesüsteemide korraldajad peaksid tagama, et nende süsteem võimaldaks ka piiriüleselt välkmakseid edastada. Euroopa Kekspank on siin võtnud südameasjaks tagada välkmaksete edastamine ka piiriüleselt ja seda aastaks 2021 lõpuks ehk tagada TARGETil põhinevale välkmaksete süsteemile (TIPS) juurdepääs kas otse või kaudselt. Kusjuures, ambitsioon on tagada mitte üksnes piiriülene välkmakse vaid ka piiriülene välkmakse mistahes majanduspiirkonna valuutas.

Ühtlasi on kavas laiendada maksesüsteemidele juurdepääsuvõimalusi ka muudele makseteenuse pakkujatele kui pangad. Komisjoni eesmärk on üle vaadata arvelduste lõplikkust käsitleva direktiivi sätted, muu hulgas kaaluda võimalusi makseasutuste ja e-rahaasutuste liitumiseks maksesüsteemidega.

Tõhusamalt toimivad rahvusvahelised maksed. Eesmärgil on eelkõige sotsiaalmajanduslik mõõde, millega soovitakse leevendada tõrkeid raha ülekandmisel (sh rahasiire) EL-st nö madala sissetulekuga riikidesse väljaspool Euroopat ja muuta raha ülekandmine mugavamaks, odavamaks ja kiiremaks.

Strateegiadokumendi kohaselt kaalutakse võimalusi liitmaks välkmakse maksesüsteeme sarnaste süsteemidega väljapool ELi tingimusel, et rakendatakse samaväärseid turvalisuse, isikuandmete kaitse ning rahapesu ja terrorismi rahastamise tõkestamise nõudeid. Samuti seda, millistel tingimusel on võimalik kolmandatel riikidel liituda SEPA[7]-ga.

Mõju Eestile: *Kavandatavad regulatiivsed muudatused aitavad kaasa innovaatiliste makseteenuste arendamisele, aitavad parandada teenuste kättesaadavust ning tagada õiglase konkurentsi läbi ühtse ja ühetaolise õigusraamistiku. Eestis on olemas võimekus välkmaksete vastuvõtmiseks ja täitmiseks. Saame üldjuhul toetada Euroopa üleselt seatud eesmärke ja oleme valmis neid rakendama, kuid saame täpsemalt mõjusid hinnata juba konkreetsete regulatiivsete ettepanekute põhjal.*

Mõju turuosalistele*: [palume sisendit]*

2.3 KRÜPTOVARATURUD

Digitaalse rahanduse paketi üks osa on kehtestada EL tasemel ühtsed nõuded krüptovarade reguleerimiseks. Nimetatud määruse kohaldumisalasse kuuluksid ettepaneku kohaselt kõik krüptovarad, mida ei ole veel ELi õigusega hõlmatud (*ehk mis ei ole finantsinstrumendid või investeerimishoius MiFID II tähenduses, e-raha EMD2 tähenduses, hoius hoiuste tagamise skeemide direktiivi tähenduses või väärtpaberistamine väärtpaberistamise direktiivi tähenduses*), ja stabiilsed mündid ehk nn "stablecoinid", ja siis eelnimetatud krüptovarade emiteerimise ja käitlemisega seotud teenuseosutajad. Mis puudutab konkreetseid nõudeid, siis krüptovara emitentidele olulisi muudatusi ei kaasne – kohustuslikuks tehakse põhiteabedokumendi (*white paper)*, mille sisu peab vastama määruse nõuetele, avalikustamine, aga järelevalveasutused ei kontrolliks selle sisu. Kõige rangemalt on reguleeritud e-raha tokenid ja varapõhised tokenid (*asset-referenced tokens*), mille puhul peab emitent taotlema tegevusloa ning saama oma instrumendi põhiteabedokumendile eelneva heakskiidu.

Lisaks krüptovarasid reguleerivale määrusele avaldas Komisjon ka hajusraamatusüsteemidel põhineva turuinfrastruktuuride pilootrežiimi määruse kavandi. Selle algatusega soovitakse edendada krüptograafilisel kujul esitatud MiFID väärtpaberite arendamist ja kasutuselevõttu ning anda võimalus tutvuda sellisel kujul esitatud väärtpaberite käibega. Pilootrežiim annab võimaluse hajusraamatu infrastruktuuridel (mitmepoolne kauplemiskoht MIFID 2 mõistes ja väärtpaberiarveldussüsteem CSDR mõistes) taotleda MiFID II ja CSDR-ist tulenevate nõuete mitte-kohaldamist.

Proportsionaalsus:
Kavandatav määrus eristab krüptovaradega seotud teenuste ja tegevuste liike vastavalt nendega seotud riskidega, et määrusega kaasnev halduskoormus oleks kaasnevate riskidega võrdelises seoses. Lisaks, määruses sätestatud nõuded on proportsionaalsed seotud riskidega, arvestades suhteliselt väikest turu suurust. Samal ajal kehtestatakse määrusega rangemad nõuded nn *stablecoin*'idele, mis suure tõenäosusega saavutavad kiiremini suurema kasutusulatuse ja millega ilmselt kaasneb suurem risk investoritele, tehingu vastaspooltele ja finantssüsteemile.

I jaotis: määruse sisu, kohaldumisala ja mõisted.

Kavandatava määruse **I jaotuses** sätestatakse selle **sisu, kohaldumisala ja mõisted. Artikkel 1** sedastab määruse sisu, milleks on:
1) luua ühtsed ja läbipaistvad reeglid krüptovarade väljastamisele ja kauplemisele võtmise kohta;
2) sätestada tegevusloa väljastamise tingimused ja järelevalve alused krüptovarateenuste osutajatele ja varapõhiste ning e-raha tokenite väljastajatele;
3) tarbijakaitsereeglite kehtestamine krüptovarade väljastamisele, kauplemisele, vahetamisele ja hoiustamisteenuste osutajatele;

[7] Single European Payment Area

4) turukuritarvitamise meetmete kehtestamine, millega soovitakse tagada krüptovara turgude ühtsus ja terviklikkus.

Artikkel 2 sätestab kohaldamisala, mis hõlmab juriidilisi isikuid, kes väljastavad krüptovarasid, kes osalevad krüptovarade väljastamises või kes osutavad krüptovaradega seotud teenuseid.

Samuti **sätestatakse erandid** (artikkel 2 punkt 2), millest tulenevalt ei kohaldata käesolevat määrust:
1) finantsinstrumentidele direktiivi 2014/65/EL (MiFID II) artikli 4 punkti 1(15) tähenduses ehk üleantavatele väärtpaberitele, rahaturuinstrumentidele, optsioonidele, futuuridele, tuletisinstrumentidele jne;
2) e-rahale e-raha direktiivi tähenduses;
3) hoiustele direktiivi 2014/49/EL tähenduses;
4) struktureeritud hoiustele MiFID II artikli 4 punkti 1(43) tähenduses;
5) väärtpaberistamisele väärtpaberistamise määruse 2017/2402 tähenduses;
6) Euroopa Keskpangale, Euroopa Investeerimispangale ja riiklikele keskpankadele;
7) rahvusvahelistele avalikele ühendustele;
8) isikutele, kes osutavad krüptovarateenuseid ainult nendega samasse konsolideerimisgruppi kuuluvatele isikutele.

Artikkel 3 sätestab **mõisted ja nende määratlused,** mida kasutatakse käesoleva määruse tähenduses, sh „**hajusraamatutehnoloogia**“, „**krüptovara**“, „**varapõhine token**“, „**e-raha token**“, „**krüptovara teenus**“ ja „**krüptovara teenuseosutaja**“. Lisaks võib komisjon vastu võtta delegeeritud õigusakte, et täpsustada määruses sätestatud mõistete tehnilisi aspekte, arvestades turu- ja tehnoloogilisi arenguid.

Nimetatud mõisted on määruses defineeritud järgnevalt:
- „**hajusraamatutehnoloogia**“ (ehk „**DLT**“) tähendab tehnoloogia liiki, mis toetab krüpteeritud andmete hajutatud hoiustamist;
- „**krüptovara**“ on digitaalsel kujul esindatud väärtuste või õiguste kogum, mida võib üle anda ja hoiustada elektrooniliselt, kasutades hajusraamatu- või muud sarnast tehnoloogiat;
- „**varapõhine token**“ on krüptovara tüüp, mis hoiab stabiilsena oma väärtust ning mis on tagatud mitme riikliku valuutaga, ühe või mitme börsil kaubeldava toormega, ühe või mitme krüptovaraga või mitme eelnimetatud varatüübiga;
- „**e-raha token**“ on krüptovara tüüp, mis on mõeldud maksevahendina kasutamiseks ja mis tuletab oma stabiilse väärtuse ühe riikliku valuuta kaudu;
- „**krüptovara teenus**“ tähendab ükskõik millist alljärgnevat teenust või tegevust:

1) **Vara haldamise teenus (sh rahakotiteenus);**
2) **Kauplemisplatvormi haldamine;**
3) **Virtuaalvääringu vahetamise teenused;**
4) **Korralduste täitmine;**
5) **Krüptovarade pakkumise korraldamine;**
6) **Korralduste vastuvõtmine ja edastamine;**
7) **Krüptovarade osas (investeerimis)nõustamine.**

Seoses kavandatava määruse I jaotuses tooduga on komisjon selgitanud, et määruse kohaldamisalasse kuuluvad eeskätt selliste instrumentide väljastamine ja nimetatud instrumentidega seotud teenused, mis teistes EL õigusaktides on praegusel ajal reguleerimata. Seetõttu on jäetud ka määruses kasutatav „krüptovara“ mõiste laiapõhjaliseks, et hõlmata võimalikult suurel hulgal turul olevaid ja tulevikus väljastatavaid krüpto-instrumente. Lisaks tasub märkida, et määrust kohaldatakse ainult juriidilistele isikutele, kes väljastavad krüptovarasid või osutavad krüptovaradega seotud teenuseid. Seetõttu on määruse kohaldamisalast väljas näiteks sellised krüptovarad, mille puhul ei ole võimalik tuvastada nende väljastajat (sh bitcoin).

II jaotis: krüptovarade, mis ei ole varapõhised või e-raha tokenid, pakkumisele kohalduvad nõuded.

Artiklis 4 sätestatakse nõuded selliste krüptovarade, mis ei ole varapõhised või e-raha tokenid, pakkumisele. Artikli **punkt 1** kohaselt ei tohi krüptovarade väljastaja pakkuda krüptovarasid avalikkusele või taotleda selliste krüptovarade kasutuselevõttu krüpto-kauplemisplatvormil, välja arvatud juhul, kui selliste krüptovarade väljastaja on juriidiline isik, kes on koostanud määruse nõuetele vastava põhiteabedokumendi, selle dokumendi esitanud teadmiseks kohalikule järelevalveasutusele ning dokumendi ka avalikustanud. Sama artikkel sätestab ka erandid,

st **punkt 2** kohaselt ei kohaldata krüptovarade pakkumisele muid nõudeid peale juriidilise isiku vormi, kui: **krüptovarasid pakutakse tasuta**, kui **krüptovarad väljastatakse automaatselt vastutasuna kaevandamise ning hajusraamatusüsteemi tööshoidmise eest**; kui pakutavad krüptovarad on **unikaalsed ning äravahetamatud teiste krüptovaradega**; kui **pakkumine on suunatud vähem kui 150 isikule liikmesriigi kohta**; kui pakkumise **koguväärtus on alla EUR 1 mio** kõikide liikmesriikide kohta; või kui pakkumine on **suunatud ainult kutselistele investoritele** ja **krüptovarasid saavad omada ainult nimetatud kutselised investorid**. Sama artikli **punktiga 3** on seatud ka piirang krüptovarade pakkumisele – pakkumine ei tohi kesta kauem kui 12 kuud.

Artiklis 5 on kirjeldatud täpsemalt krüptovara põhiteabedokumendi üksikasju ja sisu, samuti vormi ja muid nõudeid. Põhiteabedokument peaks tagama investorile võimaluse teha teadlik investeerimisotsus temale esitatud teabe põhjal. Seetõttu peaks põhiteabedokument sisaldama üksikasjalikku krüptovarade väljastaja kirjeldust ning peamisi projektis osalejaid, pakutava krüptovara ning pakkumise detailset kirjeldust, mis selgitab pakutava krüptovara olemust ning pakkumise tingimusi. Samuti tuleb põhiteabedokumendis ära märkida kasutatava tehnoloogia iseärasused, pakkumisega kaasnevad riskid ning õigused ja kohustused, mis krüptovara omamisega kaasnevad. Lisaks tuleb tagada, et põhiteabedokumendis esitatud teave on esitatud ausal ja mitte-eksitaval viisil ning et teave oleks esitatud lihtsasti arusaadaval moel. Viimaks tuleb põhiteabedokumendis välja tuua selge teade, mille kohaselt krüptovarad võivad osaliselt või täielikult oma väärtuse kaotada, krüptovarad ei pruugi olla üleantavad või likviidsed, ning kasutustokenite puhul ei pruugi neid saada vahetada reklaamitud toote või teenuse vastu, eriti juhul, kui krüptovarade pakkumisega seotud (äri)projekt luhtub või hoopis lõpetatakse.

Artikkel 6 kehtestab nõuded **turundusteabele,** sealhulgas **reklaamteadetega seotud nõuded**. Selle kohaselt tuleb krüptovarasid avalikkusele pakkudes selgelt eristada reklaamteateid muust pakkumisega seotud teabest, pakkumise teave peab olema aus, selge ja mitte-eksitav; turundusteabes esitatud teave peab ühtima põhiteabedokumendis sätestatuga ning avaldatud reklaamteave peab sisaldama viidet avalikustatud põhiteabedokumendile.

Artikkel 7 sätestab krüptovara põhiteabedokumendi teadmiseks esitamise nõuded. Nimelt tuleb enne pakkumise avalikustamist esitada põhiteabedokument asukohajärgsele liikmesriigi finantsjärelevalveasutusele vähemalt 20 päeva enne pakkumise alguskuupäeva, kuid põhiteabe-dokumendi sisu heakskiitmise nõudmine finantsjärelevalveasutuse poolt ei ole lubatud (**punktid 1** ja **2)**. Koos põhiteabedokumendiga tuleb esitada ka analüüs, miks pakutavat krüptovara ei käsitleta väärtpaberina, hoiusena, e-rahana või struktureeritud hoiusena, ning liikmesriikide loetelu, kus krüptovara plaanitakse pakkuda (**punktid 3** ja **4**). **Punkti 5** kohaselt esitab liikmesriigi järelevalveasutus saadud põhiteabedokumendid teadmiseks ESMA-le.

Artiklid 8 kuni **11** kirjeldavad krüptovara pakkumise erinõudeid ning põhiteabedokumendi muutmist. **Artikli 8 punktide 1** ja **2** kohaselt tuleb põhiteabedokument avalikustada pakkuja veebilehel hiljemalt pakkumise alguskuupäevaks, ning avalikustatud põhiteabedokument peab olema identne selle dokumendiga, mis varasemalt esitati finantsjärelevalveasutusele teadmiseks. **Artikli 9** kohaselt tuleb pakkumise lõppkuupäevast (kui lõppkuupäev on eelnevalt kindlaks määratud) arvates 16 tööpäeva jooksul avalikustada pakkumise tulemused (**punkt 1**). Samuti tuleb ette näha krüptovara pakkumise vältel kaasatud varade turvaline hoiustamine, st kaasatud riiklikud valuutad tuleb hoiustada krediidiasutuses ja kaasatud krüptovarad tuleb hoiustada tegevusloaga krüptovarateenuse osutaja juures.

Artiklis 10 on täpsustatud, et pärast põhiteabedokumendi avalikustamist võib krüptovarade väljastaja pakkuda krüptovarasid liiduüleselt ning taotleda nimetatud krüptovarade kauplemisele võtmist kauplemisplatvormil (**punkt 1**). Sama artikli **punkt 2** keelab täiendava teabe nõudmist sellistelt krüptovara väljastajatelt, kes on põhiteabedokumendi avalikustanud.

II jaotis sisaldab ka erisätteid krüptovara omandajale antud 14-päevase taganemisõiguse kohta (**artikkel 12**), kõigile krüptovara emitentidele kehtestatud kohustuste kohta (**artikkel 13**) ning emitendi vastutuse kohta seoses krüptovara põhiteabedokumendiga (**artikkel 14**).

III jaotis: varapõhiste tokenite pakkumisele kehtestatud nõuded.

III jaotise 1. peatükis kirjeldatakse varapõhiste tokenite emitentidele tegevusloa andmise menetlust ja nende krüptovara põhiteabedokumendi heakskiitmist riigi pädeva asutuse poolt (**artiklid 16–19** ning **määruse I ja II lisa**). Selleks, et saada luba liidus tegutsemiseks, peavad varapõhiste tokenite emitendid olema asutatud ELis

juriidilise isikuna (**artikkel 15**). **Artiklis 15** on samuti sätestatud, et varapõhiseid tokeneid ei tohi liidus avalikult pakkuda ega krüptovaradega kauplemise platvormil kauplemisele lubada, kui emitendil ei ole liidus tegevusluba ja ta ei avalda krüptovara põhiteabedokumenti, mille on heaks kiitnud pädev asutus. **Artikkel 15** sisaldab ka erandeid väikesemahulistele varapõhistele tokenitele ja sellistele varapõhistele tokenitele, mida turustavad, levitavad ja omavad üksnes kutselised investorid. Tegevusloa kehtetuks tunnistamist on üksikasjalikult kirjeldatud **artiklis 20** ning krüptovara põhiteabedokumendi muutmise kord on sätestatud **artiklis 21**.

III jaotise 2. peatükis on sätestatud varapõhiste tokenite emitentide kohustused. Seal on sätestatud, et nad tegutsevad ausalt, õiglaselt ja professionaalselt (**artikkel 23**). Seal on sätestatud ka krüptovara põhiteabedokumendi ja võimalike reklaamteadete avaldamise eeskirjad (**artikkel 24**) ning nende teadete suhtes kohaldatavad nõuded (**artikkel 25**). Lisaks kehtivad emitentidele jooksvad teavitamiskohustused (**artikkel 26**) ja nad peavad kehtestama kaebuste käsitlemise korra (**artikkel 27**).

Samuti peavad nad täitma muid nõudeid, mis puudutavad huvide konflikte (**artikkel 28**), pädeva asutuste teavitamist juhtorgani muutustest (**artikkel 29**), juhtimiskorda (**artikkel 30**), omavahendeid (**artikkel 31**), varapõhiste tokenite reservvarasid (**artikkel 32**) ja reservvarade hoidmist (**artikkel 33**). **Artiklis 34** selgitatakse, et emitent investeerib reservvarasid üksnes varadesse, mis on turvalised, madala riskiga varad. **Artikliga 35** kehtestatakse varapõhiste tokenite emitentidele kohustus avalikustada varapõhiste tokenitega kaasnevad õigused, sh mis tahes otsene nõudeõigus emitendi või reservvarade suhtes. Kui varapõhiste tokenite emitent ei paku kõigile varapõhiste tokenite omanikele otsest tagastamisõigust ega nõudeõigusi emitendi või reservvarade suhtes, annab artikkel 35 varapõhiste tokenite omanikele minimaalsed õigused. **Artikliga 36** keelatakse varapõhiste tokenite emitentidel ja krüptovarateenuse osutajatel maksta varapõhiste tokenite omanikele intresse.

III jaotise 4. peatükis on sätestatud eeskirjad varapõhiste tokenite emitentide omandamise kohta, kusjuures **artiklis 37** on kirjeldatud kavandatava omandamise hindamist ja **artiklis 38** sellise hindamise sisu.

III jaotise 5. peatükis (**artiklis 39**) on sätestatud kriteeriumid, mille põhjal EBA otsustab, kas varapõhine token on oluline. Need kriteeriumid on järgmised: varapõhiste tokenite turustajate kliendibaasi suurus, varapõhiste tokenite väärtus või turukapitalisatsioon, tehingute arv ja väärtus, reservvarade maht, emitentide piiriülese tegevuse olulisus ja seotus finantssüsteemiga. **Artikliga 39** antakse ka komisjonile volitused võtta vastu delegeeritud õigusakt, et täpsustada asjaolusid ja künniseid, mille puhul varapõhiste tokenite emitenti peetakse oluliseks. Artikkel 39 sisaldab mõningaid miinimumkünniseid, mida delegeeritud õigusakt peab igal juhul järgima.

Artiklis 40 on kirjeldatud varapõhiste tokenite emitendi võimalust liigitada end tegevusloa taotlemise ajal omal algatusel oluliseks. **Artiklis 41** on loetletud täiendavad kohustused, mida kohaldatakse oluliste varapõhiste tokenite emitentide suhtes, näiteks täiendavate omavahendite nõue, likviidsuse juhtimise põhimõtted ja koostalitlusvõime.

III jaotise 6. peatükis (**artiklis 42**) kohustatakse emitenti kehtestama oma tegevuse nõuetekohase lõpetamise kord.

IV jaotise 1. peatükis kirjeldatakse e-raha tokenite emitendile tegevusloa andmise menetlust.

Artiklis 43 on sätestatud, et liidus ei tohi e-raha tokeneid avalikult pakkuda ega neid krüptovaradega kauplemise platvormil kauplemisele lubada, v.a juhul, kui emitent on tegevusloa saanud krediidiasutus või e-raha asutus direktiivi 2009/110/EÜ artikli 2 punkti 1 tähenduses. **Artiklis 43** on samuti sätestatud, et e-raha tokenid on e-raha direktiivi 2009/110/EÜ tähenduses.

Artiklis 44 kirjeldatakse, kuidas e-raha omanikele antakse emitendi suhtes nõudeõigus: e-raha tokenid antakse välja nimiväärtuses ja rahaliste vahendite saamisel; e-raha tokenite omaniku taotlusel peab emitent need igal ajal nimiväärtuses tagasi ostma. **Artikliga 45** keelatakse e-raha tokenite emitentidel ja krüptovarateenuse osutajatel maksta e-raha tokenite omanikele intresse. **Artiklis 46** ja **III lisas** on sätestatud nõuded e-raha tokenite emiteerimisega kaasnevale krüptovara põhiteabedokumendi, näiteks: emitendi kirjeldus, emitendi projekti üksikasjalik kirjeldus, märge selle kohta, kas tegemist on e-raha tokenite avaliku pakkumise või kauplemisplatvormil kauplemisele lubamisega, samuti teave e-raha emitendiga seotud riskide, e-raha tokenite ja mis tahes võimaliku projekti elluviimise kohta. **Artikkel 47** sisaldab sätet e-raha tokenitega seotud krüptovara põhiteabedokumendi kaasneva vastutuse kohta. **Artiklis 48** on sätestatud nõuded e-raha tokenite pakkumisega

seotud võimalike reklaamteadete kohta ning **artiklis 49** on sätestatud, et kõik rahalised vahendid, mida emitent saab e-raha tokenite eest, investeeritakse samas vääringus nomineeritud varadesse, millel põhineb e-raha token.

IV jaotise 2. peatükis (**artiklis 50**) on sätestatud, et EBA liigitab e-raha tokenid oluliseks artiklis 39 loetletud kriteeriumide alusel. **Artiklis 51** on kirjeldatud e-raha tokenite emitendi võimalust liigitada end tegevusloa taotlemise ajal omal algatusel oluliseks. **Artikkel 52** sisaldab täiendavaid kohustusi, mida kohaldatakse oluliste e-raha tokenite emitentide suhtes. Oluliste e-raha tokenite emitendid peavad kohaldama artiklit 33 reservvarade hoidmise kohta ja artiklit 34 nende varade investeerimise kohta direktiivi 2009/110/EÜ artikli 7 asemel, artikli 41 lõikeid 1, 2 ja 3 tasustamise, koostalitlusvõime ja likviidsuse juhtimise kohta, artikli 41 lõiget 4 direktiivi 2009/110/EÜ artikli 5 asemel ja artiklit 42 tegevuse nõuetekohase lõpetamise kohta.

V jaotis sisaldab sätteid krüptovarateenuse osutajate tegevuslubade ja tegutsemistingimuste kohta.

1. peatükis määratletakse tegevusloa taotlemist käsitlevad sätted (**artikkel 53**), täpsustatakse sellise taotluse sisu (**artikkel 54**), taotluse hindamist (**artikkel 55**) ja pädevatele asutustele tegevusloa kehtetuks tunnistamiseks antud õigusi (**artikkel 56**). Peatükis antakse ESMA-le volitus luua kõigi krüptovarateenuse osutajate register (**artikkel 57**), mis sisaldab ka teavet pädevate asutuste poolt esitatud teavet krüptovara põhiteabedokumentide kohta. Krüptovarateenuste piiriülese osutamise puhul sätestatakse **artiklis 58** üksikasjad ja viis, kuidas päritoluliikmesriigi pädev asutus peaks edastama vastuvõtva liikmesriigi pädevale asutusele teavet krüptovaraga seotud piiriülese tegevuse kohta.

2. peatükis kehtestatakse nõuded kõigile krüptovarateenuse osutajatele, näiteks kohustus tegutseda ausalt, õiglaselt ja professionaalselt (**artikkel 59**), usaldatavusnõuete kohased kaitsemeetmed (**artikkel 60** ja **IV lisa**), organisatsioonilised nõuded (**artikkel 61**), klientide krüptovarade ja rahaliste vahendite hoidmise eeskirjad (**artikkel 63**), kaebuste käsitlemise korra kehtestamise kohustus (**artikkel 64**), huvide konflikti käsitlevad eeskirjad (**artikkel 65**) ja tegevuse edasiandmise eeskirjad (**66**).

V jaotise 3. peatükis on sätestatud nõuded konkreetsetele teenustele: krüptovara hoidmine (**artikkel 67**), krüptovaradega kauplemise platvormid (**artikkel 68**), krüptovara vahetamine usaldusraha või muu krüptovara vastu (**artikkel 69**), korralduste täitmine (**artikkel 70**), krüptovara suunatud pakkumine (**artikkel 71**), korralduste vastuvõtmine ja edastamine kolmandate isikute nimel (**artikkel 72**) ning krüptovara kohta nõu andmine (**artikkel 73**). 4. peatükis täpsustatakse krüptovarateenuse osutajate omandamise eeskirju.

VI jaotises kehtestatakse keelud ja nõuded, et vältida turu kuritarvitamist seoses krüptovaradega. **Artiklis 76** määratakse kindlaks turu kuritarvitamist käsitlevate eeskirjade kohaldamisala. **Artiklis 77** määratletakse siseteabe mõiste ja sätestatakse, et emitent, kelle krüptovara on lubatud krüptovaradega kauplemise platvormil kauplemisele, avalikustab siseteabe. Muudes selle jaotise sätetes keelustatakse siseteabe alusel kauplemine (**artikkel 78**), siseteabe ebaseaduslik avalikustamine (**artikkel 79**) ja turuga manipuleerimine (**artikkel 80**).
VII jaotises on esitatud üksikasjad riikide pädevate asutuste, EBA ja ESMA volituste kohta.

VII jaotise 1. peatükis kehtestatakse liikmesriikidele kohustus määrata käesoleva määruse kohaldamiseks üks või mitu pädevat asutust, sh üks pädev asutus, mis tegutseb ühtse kontaktpunktina (**artikkel 81**). Samuti on 1. peatükis esitatud üksikasjalikud sätted riikide pädevate asutuste volituste kohta (**artikkel 82**), pädevate asutuste omavahelise koostöö kohta (**artikkel 83**) ning nende koostöö kohta ESMA ja EBAga (**artikkel 84**) või muude asutustega (**artikkel 85**). Samuti kirjeldatakse üksikasjalikult liikmesriikide teatamiskohustusi (**artikkel 86**), ametisaladuse eeskirju (**artikkel 87**), andmekaitset (**artikkel 88**) ning ettevaatusabinõusid, mida võivad võtta vastuvõtva liikmesriigi pädevad asutused (**artikkel 89**). **Artiklis 90** sätestatakse eeskirjad koostööks kolmandate riikidega ja **artiklis 91** täpsustatakse kaebuste käsitlemist pädevate asutuste poolt.

VII jaotise 2. peatükis kirjeldatakse üksikasjalikult halduskaristusi ja -meetmeid, mida pädevad asutused võivad kehtestada (**artikkel 92**), nende järelevalve- ja karistuste määramise volituste kasutamist (**artikkel 93**), edasikaebamise õigust (**artikkel 94**), otsuste avaldamist (**artikkel 95**), karistustest teatamist ESMA-le ja EBA-le (**artikkel 96**) ning rikkumistest teatamist ja rikkumistest teatavate isikute kaitset (**artikkel 97**).

VII jaotise 3. peatükis on üksikasjalikud sätted EBA volituste ja pädevuste kohta seoses oluliste varapõhiste tokenite ja oluliste e-raha tokenite emitentide järelevalvega, sh järelevalvekohustused (**artikkel 98**) ning eeskirjad oluliste varapõhiste tokenite emitentide järelevalvekolleegiumide kohta (**artikkel 99**). Kolleegium koosneb muu hulgas selle päritoluliikmesriigi pädevast asutusest, kus varapõhiste tokenite emitendile on antud tegevusluba,

EBAst, ESMAst, pädevatest asutustest, kes teevad järelevalvet kõige olulisemate krüptovaradega kauplemise platvormide üle, reservvarade hoidjatest, krediidiasutustest jt, kes osutavad teenuseid seoses olulise varapõhise tokeniga, ning EKPst. Kui oluliste varapõhiste tokenite emitent on asutatud liikmesriigis, mille raha ei ole euro, või kui reservvarade hulka kuulub vääring, mis ei ole euro, kuulub ka selle liikmesriigi keskpank kolleegiumi koosseisu. Kolleegiumisse mittekuuluvad pädevad asutused võivad taotleda kolleegiumilt kogu teavet, mida on vaja nende järelevalveülesannete täitmiseks. **Artiklis 99** kirjeldatakse ka seda, kuidas EBA peab koostöös ESMA ja Euroopa Keskpankade Süsteemiga töötama välja regulatiivsete standardite eelnõud, et määrata kindlaks kõige asjakohasemad kauplemisplatvormid ja reservvarade hoidjad, ning kolleegiumi töökorra üksikasju.

Artiklis 100 antakse kolleegiumile volitused esitada mittesiduvaid arvamusi. Need arvamused võivad olla seotud nõudega, et emitendil peab olema suurem summa omavahendeid, muudetud krüptovara põhiteabedokumendiga, tegevusloa kavandatava kehtetuks tunnistamisega, kavandatava teabevahetuslepinguga kolmanda riigi järelevalveasutusega jne. Olulise e-raha tokeni emitendi pädev asutus või EBA kaalub nõuetekohaselt kolleegiumi arvamusi ja kui nad ei ole selle arvamusega – sh mis tahes soovitustega – nõus, peab nende lõplik otsus sisaldama selgitusi iga olulise kõrvalekalde kohta arvamusest või soovitustest.

Artiklis 101 sätestatakse oluliste e-raha tokenite emitentide järelevalvekolleegiumide eeskirjad. Need kolleegiumid toimivad samamoodi nagu varapõhiste tokenite kolleegiumid (täiendavate osalejate hulka kuuluvad oluliste e-raha tokenitega seoses makseteenuseid osutavate kõige olulisemate makseasutuste pädevad asutused). **Artiklis 102** sätestatakse kolleegiumi volitused esitada mittesiduvaid arvamusi.

4. peatükis on sätestatud EBA volitused ja pädevus seoses oluliste varapõhiste tokenite ja oluliste e-raha tokenite emitentidega. Ametisaladus (**artikkel 103**), teabenõue (**artikkel 104**), üldised uurimisvolitused (**artikkel 105**), kohapealne kontroll (**artikkel 106**), teabevahetus (**artikkel 107**), kokkulepe teabevahetuseks kolmandate riikidega (**artikkel 108**), kolmandatest riikidest saadud teabe avaldamine (**artikkel 109**) ja koostöö teiste asutustega (**artikkel 110**). Ametisaladuse hoidmise kohustust on nimetatud **artiklis 111** ja EBA järelevalvemeetmeid **artiklis 112**. Halduskaristused ja muud meetmed, eelkõige trahvid, on üksikasjalikult sätestatud **artiklis 113**, kusjuures järgnevad artiklid käsitlevad perioodilisi karistusmakseid (**artikkel 114**), trahvide avalikustamist, laadi ja jõustamist (**artikkel 115**) ning vastavaid menetluseeskirju järelevalvemeetmete võtmiseks ja trahvide määramiseks (**artikkel 116**). **Artiklites 117** ja **118** on sätestatud vastavalt asjaomaste isikute ärakuulamise nõuded ja Euroopa Kohtu täielik pädevus vaadata läbi EBA otsuseid. Kooskõlas **artikliga 119** peaks EBA-l olema määruse kohaselt vastu võetud delegeeritud õigusakti alusel võimalik võtta oluliste varapõhiste tokenite emitentidelt ja oluliste e-raha tokenite emitentidelt tasusid. **Artikliga 120** antakse EBA-le volitused delegeerida konkreetseid järelevalveülesandeid pädevatele asutustele, kui seda on vaja olulise varapõhise tokeni emitendi või olulise e-raha tokeni emitendi nõuetekohaseks järelevalveks.

Volituste delegeerimist eesmärgiga võtta vastu komisjoni delegeeritud õigusakte on käsitletud **VIII jaotises**. Määruse ettepanek sisaldab komisjonile antud volitusi võtta vastu delegeeritud õigusakte, milles täpsustatakse teatavaid üksikasju, nõudeid ja korda, nagu on määruses sätestatud (**artikkel 121**).

IX jaotis sisaldab ülemineku- ja lõppsätteid, sh komisjoni kohustust koostada aruanne, milles hinnatakse määruse mõju (**artikkel 122**). **Artiklis 123** loetletud üleminekumeetmed sisaldavad klauslit, mis käsitleb varem kehtinud nõuete kohaldamist enne käesoleva määruse jõustumist emiteeritud krüptovarade, v.a varapõhiste tokenite ja e-raha tokenite suhtes. **Artikliga 124** muudetakse direktiivi liidu õiguse rikkumisest teatavate isikute kaitse kohta (direktiiv (EL) 2019/1937), lisades sellesse käesoleva määruse, ning **artiklis 125** täpsustatakse, et see muudatus tuleb siseriiklikku õigusesse üle võtta 12 kuu jooksul pärast käesoleva määruse jõustumist. **Artiklis 126** on sätestatud, et käesolevat määrust hakatakse kohaldama 18 kuud pärast selle jõustumist, v.a e-raha tokenite ja varapõhiste tokenitega seotud sätteid, mida hakatakse kohaldama käesoleva määruse jõustumise kuupäeval.

Mõju Eestile. *Positiivsete mõjudena võib välja tuua, et tõhustatakse investorkaitse nõudeid ja tekib parem ülevaade virtuaalvaradega seotud teenuseid pakkuvatest isikutest ja asjaomasest turust tervikuna.*

Kavandatavad muudatused mõjutavad Finantsinspektsiooni järelevalvelist tegevust, kuna inspektsioon peab teostama järelevalvet ka määruses sätestatud nõuete täitmise üle ning see eeldab spetsiifilisi teadmisi virtuaalvaradest ja nendega seotud tehnoloogilistest aspektidest. [Palume Finantsinspektsiooni sisendit]

***Mõjud RAB**-ile: Määruses välja pakutu puhul on krüptovarateenuste näol pigem tegemist Finantsinspektsiooni järelevalve alla kuuluva teenusega, mis tähendab, et virtuaalvääringu teenustega seotud järelevalve tuleb Eesti õiguses ümber korraldada. Sellega seoses väheneks ka RAB-i halduskoormuse maht, mis suureneks samaaegselt Finantsinspektsioonil.*
[Palume Rahapesu Andmebüroo (täiendavat) sisendit]

***Mõju teistele turuosalistele**: [palume sisendit]*

2.4 HAJUTUSRAAMATU TEHNOLOOGIAL PÕHINEV TURUINFRASTRUKTUURIDE KAITSEREŽIIM

Käesoleva algatusega soovitakse edendada krüptograafilisel kujul esitatud MiFID väärtpaberite arendamist ja kasutuselevõttu ning anda võimalus tutvuda sellisel kujul esitatud väärtpaberite käibega. Pilootrežiim annab võimaluse hajusraamatu infrastruktuuridel (pilootprojekt on suunatud kahele turu-osalisele - mitmepoolne kauplemiskoht MIFID II mõistes ja väärtpaberiarveldussüsteem CSDR mõistes) taotleda mõjuval põhjusel MiFID II ja CSDR-ist tulenevate nõuete mitte-kohaldamist, edendamaks finantssektoris hajusraamatusüsteemide kasutuselevõttu. Mõjuva põhjuse all peetakse silmas olemas-olevatest eelviidatud direktiivist ja määrusest tulenevaid nõudeid, mis takistavad väärtpaberite registreerimist ja kauplemist hajusraamatutehnoloogial (edaspidi **DLT**) põhinevatel infrastruuridel. Pilootprojektis osalemine on vabatahtlik, erandite andmist otsustab finantsjärelevalveasutus (meil Finantsinspektsioon).

Artiklis 1 on sätestatud määruse reguleerimis- ja kohaldumisala. Täpsemalt sätestatakse määrusega DLT-l põhinevate turu infrastruktuuride tegutsemise tingimused, DLT-süsteemide kasutamise lubatavus ning järelevalve ja koostöö pädevate asutuste ja ESMA vahel. Määrust kohaldatakse turuosalistele (investeerimisühingud, väärtpaberituru korraldaja ning väärtpaberite keskregistrid), mis võivad taotleda luba määruse artikli 7 või 8 kohaselt.
Artikkel 2 sätestab mõisted ja definitsioonid, mille hulka kuuluvad „DLT turu infrastruktuur“, „DLT mitmepoolne kauplemissüsteem“, „DLT väärtpaberite registreerimise süsteem“ ja „DLT üleantavad väärtpaberid“.
Artiklis 3 on kirjeldatud piirangud, milliseid DLT üleantavaid väärtpabereid võib kauplemiseks võtta või registreerida DLT turu infrastruktuuride poolt. Mis puudutab aktsiaid, siis DLT üleantavate aktsiate emitendi turukapitalisatsioon peaks olema alla 200 miljoni euro, ning avalike võlakirjade puhul (mis ei hõlma riiklikke võlakirju, tagatud võlakirju ja korporatiivvõlakirju) on piirang 500 miljonit eurot. Sealjuures märgitakse, et DLT turu infrastruktuurid ei peaks võimaldama riiklike võlakirjadega kauplemist või nende registreerimist. Lisaks, üks DLT väärtpaberite arveldussüsteem ei tohiks registreerida DLT üleantavaid väärtpabereid rohkem kui kogumahus 2,5 miljardit eurot[8].
Artiklis 4 on sätestatud DLT mitmepoolse kauplemissüsteemi nõuded, mis on samad võrreldes MiFID II-ga, ning täpsustab käesoleva määrusega võimaldavaid erandeid.
Artikkel 5 sätestab väärtpaberite keskregistri nõudes, mis on samad võrreldes CSDR-iga, ning täpsustab käesoleva määrusega võimaldavaid erandeid. Artiklid 4 ja 5 sisaldavad piiratud hulgal erandeid, mille kohaldamist DLT turu infrastruktuurid saavad taotleda ning tingimused, mis erandi andmisega kaasnevad.
Artiklis 6 on sätestatud täiendavad tingimused, millele DLT infrastruktuurid peavad vastama, et pöörata rõhku uutele riskidele, mis tulenevad DLT kasutamisest. Nimelt, DLT turu infrastruktuurid peavad andma kõikidele, liikmetele, osalistele, klientidele ja investoritele selget ja üheselt mõistetavat teavet selle kohta, et kuidas teostatakse oma funktsioone, pakutakse teenuseid ja tegevusi ja kuidas need erinevad tavalisest mitmepoolsest kauplemissüsteemist või keskregistrist. DLT turu infrastruktuurid peavad ka veenduma, et neil on olemas piisavad IT ja küberturvalisuse meetmed, mis puudutab DLT kasutamist. Kui DLT turu infrastruktuuride ärimudel hõlmab

[8] Võrdluseks: Nasdaq Baltic on kauplemisele võtnud 68 äriühingu aktsiad, mille turuväärtus on kokku 7,5 mld EUR. Allikas: https://nasdaqbaltic.com/statistics/et/capitalization

ka klientide vara või DLT väärtpaberite hoidmist, või nendele ligipääsu, siis infrastruktuuridel peab olema piisavad kaitsemeetmed, et kindlustada hoiustavate varade või väärtpaberite turvalisus.
Artiklid 7 ja 8 sätestavad DLT mitmepoolse kauplemissüsteemi ja –väärtpaberiarveldussüsteemi haldamiseks spetsiifilise loa taotlemise protseduuri ning nimetavad andmed ja dokumendid, mis tuleb nimetatud loa taotlemisel esitada.
Artikkel 9 selgitab DLT turu infrastruktuuri, kohalike järelevalveasutuste ja ESMA vahelist koostööd.
Artikkel 10 märgib, et viieaastase perioodi lõppedes ESMA koostab COM-ile raporti pilootrežiimi kohta. Raporti põhjal koostab COM oma raporti, milles sisaldub kulu ja kasutegurite analüüs selle kohta, kas pilootrežiimi tuleks jätkata, muuta või lõpetada.
Artikli 11 kohaselt jõustub määrus 12 kuud pärast selle vastuvõtmist.

Mõju Eestile: *Kavandatavad muudatused mõjutavad Eesti finantsturusüsteemi eelduslikult väiksel või keskmisel määral.*

Mõju investeerimisühingutele*: Täna tegutseb turul viis investeerimisühingut, millest üks on väärtpaberituru kauplemiskoht, ja üks väärtpaberiarveldussüsteem (täpsemalt selle Eesti filiaal), ning üheksa krediidiasutust, kes võivad investeerimisteenuseid pakkuda ilma täiendava tegevusloata. Hinnanguliselt hakkab pilootprojekti võimalusi kasutama vähemalt üks eeltoodud turuosalistest või asutatakse vähemalt üks uus teenusepakkuja, kes hajusraamatusüsteemidel põhinevat tegevusplaani rakendama hakkaks.*

Kavandatud määrus on oma sisult sarnane möödunud aastatel Finantsinspektsiooni juures rakendatud nn regulatiivse liivakastiga (ingl. k regulatory sandbox), mis oli mõeldud uudsete ja innovaatiliste finantsteenuste kasutamiseks piiratud keskkonnas, kuid milles osalemise vastu oli kesine huvi ning mis seetõttu ära lõpetati. Seevastu antud pilootrežiim EL määruse toega võiks suurendada turuosaliste õiguskindlust ning viieaastane kohustuslik pilootrežiimi tööshoidmise tähtaeg innustada turuosalisi kõnesolevate hajusraamatusüsteemidel põhinevaid ärimudeleid katsetama.

Mõju teistele turuosalistele*: [palume sisendit]*

Mõju pädevatele asutustele*: [palume sisendit]*

2.5 FINANTSTEENUSTE DIGITAALNE OPERATSIOONILINE VASTUPIDAVUS

DORA peamiseks eesmärgiks on ennetada ja maandada finantssektoris esinevaid digitaalseid riske, sh küberriske, mis on tingitud järjest suuremast sõltuvusest tarkvarast ja digitaalsetest protsessidest ja mis ühtlasi tähendab ka info- ja kommunikatsioonitehnoloogiaga (edaspidi ***IKT***) seotud riskide tõusu. Et finantssektor suudaks vastu pidada igasugust tüüpi IKT-ga seotud häiretele ja ohtudele, kehtestatakse kavandatava määrusega ühtsed nõuded finantsteenuste digitaalse operatsioonilise vastupidavuse kohta ehk sektori-spetsiifilised ühetaolised nõuded IKT süsteemide turvalisusele, hõlmates ka riskijuhtimist, intsidentidest raporteerimist, vastupidavusvõime testimist ja infojagamist.

I peatükk. Üldised sätted

Määruse kohaldamisalasse kuuluvad (artikkel 2):
1) krediidiasutused;
2) makseasutused;
3) e-raha asutused;
4) investeerimisühingud;
5) krüptovarade teenuse osutajad;
6) väärtpaberite keskdepositooriumid;
7) kesksed vastaspooled;

8) kauplemiskohad;
9) kauplemisteabehoidlad;
10) alternatiivfondi fondivalitsejad;
11) fondivalitsejad;
12) aruandlusteenuse osutajad;
13) kindlustusandjad ja edasikindlustusandjad;
14) kindlustusvahendajad;
15) tööandja kogumispensioni asutused;
16) reitinguagentuurid;
17) vandeaudiitorid ja audiitorettevõtjad;
18) kriitiliste võrdlusaluste haldajad;
19) ühisrahastusteenuse osutajad;
20) väärtpaberistamise registrid;
21) IKT teenuse osutajad (III osapooled).

Proportsionaalsus:

1) leevendused (eelkõige IKT riskide juhtimise raamistiku sätetes) mikroettevõtjatele – alla 10 töötaja, kelle aastane käive ja/või bilansimaht ei ületa 2 miljonit eurot;
2) IKT riskidega seotud juhtumistest teavitamine – teavitada tuleb ainult olulistest juhtumitest;
3) kõrgemad testimise nõuded olulistele ja kübervõimekatele teenuseosutajatele;
4) järelevalve kolmandast osapoolest IKT teenuseosutajate üle – kohaldamisalasse kuuluvad ainult kriitilised IKT teenuseosutajad (DORA artikli 28 lg 2 kriteeriumitele vastavad isikud).

Mõju Eestile. *Operatsiooniliste riskide juhtimise nõuded, sh nõuded küberturvalisuse tagamiseks ei ole finantssektori jaoks midagi uut. Määrusega kehtestatavad nõuded on käesoleval ajal kaetud erinevate standardite ja seadustega. Näiteks ISO27000 standardid, suuremahulistest intsidentidest teavitamist reguleerib täna küberturvalisuse seadus, hädaolukorra seadus ja Finantsinspektsiooni juhendid (nt nõuded finantsjärelevalve subjekti infotehnoloogia ja infoturbe korraldusele), EBA suunised, SSM järelevalve. Lisaks on eurosüsteemis välja töötatud küberkerksuse ootused CROE raamistik (Cyber Resilience Oversight Expectations). Käesoleva ettepanekuga mõnevõrra konsolideeritakse olemasolevaid nõudeid, mis peaks raamistiku muutma finantsteenuste osutajatele selgemaks.*

Eesti Pangaliit *on oma tagasisides avaldanud, et suures plaanis nende jaoks midagi ei muutu ehk määrusega neile olulist mõju ei kaasne.*

Mõju audiitorbüroodele*: Määruse skoopi on hõlmatud ka audiitorbürood, kes Eestis finantsjärelevalve alla ei kuulu, kuid on finantsjärelevalve subjektid mitmetes teistes EL riikides. Teadaolevalt ei kohaldu audiitorbüroodele ka küberturvalisuse seaduse nõuded, seega on kõnealustele subjektidele tegemist uute nõuetega, millega tuleb oma tegevus vastavusse viia. [palume Audiitorkogu ja audiitorbüroode sisendit kaasnevate mõjude osas]*

Mõju IKT teenuseosutajatele*: Määruse skoobis saavad olema ka IKT teenuseosutajad, kuid suuremad mõjud kaasnevad üksnes kriitilistest teenuseosutajatest IKT teenusepakkujatele (kes pakuvad teenuseid finantssektorile). ITLi hinnangul ei ole hetkel „selgust, kui palju on Eestis ettevõtjaid, kes vastaks DORA ettepanekuga ette nähtud kriteeriumitele ja oleksid kriitilise tähtsusega.“*

Mõju teistele turuosalistele*: [palume ülejäänud turuosaliste sisendit]*

II peatükk. IKT riskide juhtimine

IKT riskide juhtimine (artikkel 4) – riskide juhtimisse kaasatakse ka juhtkond, kes peavad tagama küberhügieeni terves ettevõttes, määrama selged rollid ja vastutusalad ning samuti asjaomased investeeringud IKT riskide haldamiseks ja ka väljaõppe.

IKT riskihalduse nõuded (artiklid 5-14) – Sätestab põhinõuded riskide haldusele, milleks on tuvastada, kaitsta ja ennetada, avastada, vastata ja taastada, õppida ja areneda ning suhelda ja kommunikeerida. Ettevõtjal peavad olema paigas asjaomased IKT süsteemid ja kasutuses tööriistad, mis aitavad kaasa eelpool mainitud põhimõtete rakendamisele.

Mõju Eestile: *Kavandatavad muudatused tõhustavad kindlasti finantssektori vastupidavust digitaalsetele ohtudele.*

Mõju turuosalistele*: [palume turuosaliste sisendit]*

III peatükk. IKT riskidega seotud juhtumite haldus, klassifitseerimine ja raporteerimine

IKT-ga seotud juhtumitest teavitamine (art 15-20) – Ettepaneku kohaselt peab teenuseosutajal olema juhtimisprotsess IKT-ga seotud juhtumite monitoorimiseks ja andmete säilitamiseks, misjärel tuleb need klassifitseerida ja olulisematest intsidentidest pädevat asutust teavitada. Seega on määrusega sätestatud üldised nõuded ja erinõuded suurtest intsidentidest raporteerimisele. Viimase jaoks koostavad ESAd ka vastavad protseduurid ja andmepõhjad (*templates*). Andmete kvaliteet on mh oluline ka selleks, et hiljem teha võrdlusi ja järeldusi.

Mõju Eestile: *Kavandatavad muudatused tõhustavad finantssektori vastupidavust digitaalsetele ohtudele.*

Mõju turuosalistele*: [palume turuosaliste sisendit]*

IV peatükk. Digitaalse operatsioonilise resilientsuse testimine

Digitaalse operatsioonilise resilientsuse/vastupidavusvõime testimine (art 21-24):

1) Kehtestatakse baastestimise nõuded kõikidele finantsteenuste osutajatele, sh siis perioodilise testimise nõuded, mis aitavad olla valmis ja tuvastada nõrkuseid, puudujääke või lünkasid ja et oleks võimalik võtta koheselt ka avastatud puuduste likvideerimiseks meetmeid. Testimisnõuded on proportsionaalsed ja sõltuvad suuresti ettevõtte suurusest, pakutavatest teenustest ja kasutatavatest süsteemidest.
2) Kõrgemad testimise nõuded kohalduvad olulistele ja kübervõimekatele teenuseosutajatele – need terminid on aga alles ESAde poolt väljatöötamisel), täpselt hetkel ei tea, kes hakkaksid Eestis neid nõudeid täitma.

Mõju Eestile. *Kavandatavad muudatused tõhustavad finantssektori vastupidavust digitaalsetele ohtudele.*

Mõju turuosalistele*: [palume turuosaliste sisendit]*
Baastestimise nõuded kohalduvad kõikidele DORA subjektidele. Seetõttu finantsteenuste osutajad, kellele varasemalt ei ole nõuded kohaldunud (nt ühisrahastusteenuse osutajad), peavad oma süsteemid ja protsessid viima vastavusse testimise nõuetega. Sama on ka audiitoritega.

Mõju pädevatele asutustele*: [palume sisendit]*

Mõju Eesti Pangale: Eesti Panga strateegiline ülesanne on tõhustada finantssektori kübervastupanu võimet pakkudes Eesti finantssektorile välja eurosüsteemis välja töötatud ühtne kübertestimise raamistik TIBER-EU. 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.

V peatükk. Kolmandate osapooltega seotud IKT riskide juhtimine

Selgitame, et DORA määruses on kolmandatest osapoolest IKT teenuseosutajaga seotud nõuded põhiliselt kahes osas:

Esiteks: nõuded IKT teenuse sisseostmisele ehk mida finantsasutus peab järgima, kui valib IKT teenuseosutajat ja sõlmib temaga vastava lepingu. Need nõuded kohalduvad kõikidele finantsasutustele, sõltumata, kas IKT teenuseosutaja on kriitiline või mitte. Teatud lisanõuded on määruses juhuks, kui sisseostetav teenus on kriitiline/oluline. Seega on sihtrühmaks kõik IKT teenuseosutajad, kes finantsasutustele teenust pakuvad, kuid finantsasutustel endil on kohustus tagada, et teenust ostetakse sisse määruses ettenähtud tingimustel. Samuti tagab finantsasutus, et IKT teenuseosutaja on kaasatud teatud protsessidesse, nt *advanced testing of ICT tools, systems and processes based on threat led penetration testing*.

Sihtrühm: 'ICT third-party service provider' means an undertaking providing digital and data services, including providers of cloud computing services, software, data analytics services, data centres, but excluding providers of hardware components and undertakings authorised under Union law which provide electronic communication services as defined referred to in point (4) of Article 2 of Directive (EU) 2018/1972 of the European Parliament and of the Council

Teiseks: Euroopa-ülene järelevalve kriitilise tähtsusega ITK teenuseosutajate üle. Siia hakkaksid kuuluma sellised IKT teenuseosutajad, kes on Euroopa mõistes suured, pakkudes teenust mitmes liikmesriigis ja suurele hulgale finantsasutustele, sealjuures võetakse arvesse pakutavate teenuste süsteemset mõju ja iseloomu, finantsasutuste sõltuvust nendest teenustest. Kuna kriitilise tähtsusega IKT teenuseosutaja määratlemiseks kehtestatakse lisaks DORA üldisematele kriteeriumitele alamakt, ongi mõnevõrra ebaselge, kes lõpuks selle määratluse ja EL-ülese järelevalve alla hakkaks kuuluma. Hinnata tuleb teenuseosutajate tähtsust Euroopa tasandil ehk kas ettevõtjad ka teiste liikmesriikide finantsasutustele ja mis ulatuses teenust osutavad.

I osa. Üldnõuded kolmandate osapooltega seotud IKT riskide juhtimiseks

Asjaomased nõuded on kehtestatud selleks, et oleks tagatud hea ülevaade kolmandatest osapooltest IKT teenuseosutajatega seotud riskide kohta.

Kolmandatest osapooltest IKT teenuseosutajatega seonduvad riskid (art 25-27)

Osana IKT riskide juhtimise raamistikust peavad finantsasutused ja audiitorid juhtima ka kolmandate osapooltega seotud IKT riske seoses IKT teenuse sisseostmisega. Finantsasutus ja audiitor peab pidama *Teaberegistrit* kõikide kolmandate osapooltega sõlmitud lepingute kokkulepete kohta ja kord aastas pädevat asutust teavitama kõikidest uutest lepingutest erinevate kategooriate lõikes. Kriitiliste ja oluliste teenuste korral tuleb pädevat asutust aegsasti ette teavitada kavandatavast lepingulisest kokkuleppest. Artiklis 25 on lisaks ette nähtud eeskirjad, mida finantsasutus ja audiitor peavad järgima enne, kui kolmanda osapoolega lepingu sõlmivad. Samuti on sätestatud, millistel alustel tuleks leping lõpetada. Kuivõrd enne lepingu sõlmimist tuleb ühe osana teha kindlaks ja hinnata kõiki lepinguga seotud riske, sealhulgas võimalust, et sellised lepingulised kokkulepped võivad aidata tugevdada IKT kontsentratsiooni riski, on artiklis 26 ette nähtud eraldi säte selle hindamiseks. Artiklis 27 on reguleeritud üldised põhimõtted, mida peaks lepingu sõlmimisel arvesse võtma (mis peaksid olema lepingus kajastatud).

Mõju turuosalistele: *[palume turuosaliste sisendit]*
Kõik määruse kohaldamisalasse kuuluvad Eesti finantsasutused ja audiitorid peavad IKT teenuste sisseostmisel järgima artiklites 24-27 sätestatud nõudeid, sealhulgas pidama registrit lepinguliste kokkulepete kohta ning

teavitama vastavalt Finantsinspektsiooni ja Järelevalvenõukogu, kui kavandatakse sisse osta kriitilist või olulist IKT teenust. Kuivõrd finantssektori kehtivad õigusaktid ja suunised hõlmavad samuti nõudeid teenuste sisseostmisele, siis peavad finantsasutused juba täna järgima EL õigusest tulenevaid nõuded teenuste sisseostmisele.

***Mõju pädevatele asutustele**: [palume sisendit]*

II osa. Järelevalve kolmandatest osapooltest kriitilise tähtsusega IKT teenuseosutajate üle

Määruse ettepaneku **artiklites 28–39** nähakse ette järelevalveraamistik kriitilise tähtsusega IKT teenuseosutajate üle. Kriitilise tähtsusega IKT teenuseosutaja määratlemise kriteeriumid on sätestatud artikli 29 lõikes 2 ning ettepaneku kohaselt hakkaksid nad kuuluma Euroopa Järelevalveasutuse järelevalve alla. Kriitilse IKT teenuseosutaja määratlemisel võtavad Euroopa arvesse järgmist:

- pakutavate teenuste süsteemne mõju ja iseloom;
- finantsasutuste sõltuvus nendest teenustest;
- pakkuja asendamise võimaluse tase;
- liikmesriikide arv, kus pakutakse teenust;
- liikmesriikide arv, kus pakutakse finantsasutusele teenust.

Igale IKT teenuseosutajale määratakse *Lead Overseer*, kes siis oleks EBA, EIOPA või ESMA vastavalt sellele, millise finantssektori asutustele IKT teenuseosutaja kõige rohkem teenust osutab. Eesmärgiks on tagada, et finantssektoris kriitilist rolli täitvate tehnoloogiateenuste osutajate tegevus on Euroopaüleselt nõuetekohase järelevalve all. **Artiklis 30** on reguleeritud *Lead Overseer'i* ülesanded ja **artiklis 31** tema õigused.

Artiklites 32–34 reguleeritud sätted teabe saamise, üldiste uurimisvolituste ja kohapealse kontrolli kohta on analoogsed teistes finantssektori õigusaktides sätestatuga, kui järelevalvepädevus kuulub ESMA-le. Täiendus on see, et lisaks on ette nähtub uurimismeeskonna loomine, mis peaks assisteerima *Lead Overseer'i.* See koosneb 10 liikmest ning sinna kuuluvad nii ESA töötajad, kui ka riiklike finantsjärelevalve asutuste esindajad (kus IKT teenuseosutaja teenust osutab). Liikmetel on IKT- ja operatsiooniriskidega seotud teadmised.

Artikli 38 kohaselt tasub IKT teenuseosutaja ka järelevalvetasu.

***Mõju pädevatele asutustele:** [palume sisendit]*

***Mõju Finantsinspektsioonile:** Kavandatavad muudatused mõjutavad Finantsinspektsiooni tegevust näiteks juhul, kui kriitilise tähtsusega IKT teenuseosutaja osutab Eestis olulises ulatuses teenust ning IKT ja operatsiooniriski teadmistega Finantsinspektsiooni esindaja peaks kuuluma uurimismeeskonda, mis tähendab viidatud isikule halduskoormuse tõusu.*

***Mõju teenuseosutajatele:** [palume sisendit]*

IKT teenuseosutaja, kes osutab kriitilisi IKT teenuseid finantssektorile, hakkab edaspidi alluma ESAde järelevaatamisele. Käesoleval hetkel ei ole teada, mitu sellist teenuseosutajat Eestis on või kas üldse on. Samuti on veel „kriitilise" definitsioon[9] läbirääkimistel ja käesoleval ajal ei ole selge.

[9] *Art 28. 1. The ESAs, through the Joint Committee and upon recommendation from the Oversight Forum established pursuant to Article 29(1) shall: (a) designate the ICT third-party service providers that are **critical for financial entities**, taking into account the criteria specified in paragraph 2;*

2. The designation referred to in point (a) of paragraph 1 shall be based on all of the following criteria:
(a) the systemic impact on the stability, continuity or quality of the provision of financial services in case the relevant ICT third-party provider would face a large scale operational failure to provide its services, taking into account the number of financial entities to which the relevant ICT third-party service provider provides services;
(b) the systemic character or importance of the financial entities that rely on the relevant ICT third-party provider, assessed in accordance with the following parameters: i) the number of global systemically important institutions (G-SIIs) or other systemically important institutions (O-SIIs) that rely on the respective ICT third-party service provider; ii) the interdependence between the G-SIIs or O-SIIs referred to in point (i) and other financial entities including situations where the G-SIIs or OSIIs provide financial infrastructure services to other financial entities;

Kriitilise tähtsusega IKT teenuseosutajate kriteeriumitele vastava isiku tegevus hakkaks ettepaneku kohaselt edaspidi osaliselt kuuluma Euroopa Järelevalveasutuse järelevalve alla. Seal hulgas tuleks tasuda Euroopa Järelevalveasutusele järelevalvetasu.

IV peatükk. Info jagamise kokkulepped

Artikli 40 kohaselt võivad finantsteenuse osutajad jagada omavahel teavet küberohtude ja haavatavustega seonduva kohta. Selle eesmärgiks on sektori parem valmisolek ohtudega toimetulekuks.

Mõju teenuseosutajatele: *[palume sisendit]*
Kavandatavad muudatused annavad finantsteenuste osutajatele võimaluse vabatahtlikult intsidentidega seotud teavet vahetada. Sätestatakse õiguslik alus, mis loob kindlust ja õigusselgust, et selline tegevus on lubatud. Teenuseosutajatele sellega kohustusi ei kaasne. Mõju võib pidada positiivseks.

VII peatükk. Pädevate asutuste pädevus ja õigused

Artiklis 41 on määratletud pädevad asutused, kes teostavad määruses sätestatu üle järelevalvet (v.a kriitilisest tähtsusest IKT teenuseosutaja üle). Eesti kontekstis tähendab see, et enamikel juhtudel on pädevaks asutuseks Finantsinspektsioon, kuid kuna määruse kohaldamisalasse kuuluvad mh vandeaudiitorid ja audiitorühingud, siis Eestis on vastavaks pädevaks asutuseks audiitortegevuse järelevalve nõukogu.

Pädev asutus (artiklid 41-49) – Sätestatakse koostöö nõuded NIS direktiivi pädeva asutusega, luuakse võimalused sektoriülesteks harjutusteks, kommunikeerimiseks ja koostööks. Samuti kehtestatakse halduskaristused ja muud meetmed, kui määruse nõudeid rikutakse.

Teatud määruse valdkonnad on juba hõlmatud ESA suunistega.

Mõju pädevatele asutustele: *DORAs on määratletud pädevad asutused, kes teostavad määruses sätestatu üle järelevalvet. Eesti kontekstis tähendab see, et enamikel juhtudel on pädevaks asutuseks Finantsinspektsioon, kuid kuna määruse kohaldamisalasse kuuluvad mh vandeaudiitorid ja audiitorühingud, siis Eestis on vastavaks pädevaks asutuseks audiitortegevuse järelevalve nõukogu. Samuti sätestatakse koostöö nõuded NIS direktiivi pädeva asutusega (RIA), luuakse võimalused sektoriülesteks harjutusteks, kommunikeerimiseks ja koostööks. Samuti kehtestatakse halduskaristused ja muud meetmed, kui määruse nõudeid rikutakse.*

Mõju Finantsinspektsioonile: *[palume sisendit]*
Kavandatavad muudatused mõjutavad Finantsinspektsiooni järelevalvelist tegevust, kuna inspektsioon peab teostama järelevalvet ka määruses sätestatud nõuete täitmise üle ning see eeldab spetsiifilisi teadmisi IKT riskidest ja muudest tehnoloogilistest aspektidest.

Mõju audiitortegevuse järelevalve nõukogule*: [palume sisendit]*

(c) the reliance of financial entities on the services provided by the relevant ICT third-party service provider in relation to critical or important functions of financial entities that ultimately involve the same ICT third-party service provider, irrespective of whether financial entities rely on those services directly or indirectly, by means or through subcontracting arrangements;
(d) the degree of substitutability of the ICT third-party service provider, taking into account the following parameters: i) the lack of real alternatives, even partial, due to the limited number of ICT third-party service providers active on a specific market, or the market share of the relevant ICT third-party service provider, or the technical complexity or sophistication involved, including in relation to any proprietary technology, or the specific features of the ICT third-party service provider's organisation or activity; ii) difficulties to partially or fully migrate the relevant data and workloads from the relevant to another ICT third-party service provider, due to either significant financial costs, time or other type of resources that the migration process may entail, or to increased ICT risks or other operational risks to which the financial entity may be exposed through such migration.
(e) the number of Member States in which the relevant ICT third-party service provider provides services;
(f) the number of Member States in which financial entities using the relevant ICT third-party service provider are operating.

Lisaks, kui otsustatakse, et sama järelevalvet tuleb teostada ka audiitorbüroode üle, kes hetkel ei ole finantsjärelevalve subjektid […]. Audiitortegevuse järelevalve nõukogusse asjaomase pädevuse loomine ei oleks kindlasti mõistlik. Vaid mõne töötajaga järelevalve, mis on kitsalt suunatud audiitorettevõtjate kvaliteedikontrolli läbi viima, mis puudutab raamatupidamise aastaaruande auditit ning ülevaatust, ei oma eelpool nimetatud spetsiifilisi teadmisi IKT riskidest ja muudest tehnoloogilistest aspektidest. Vastava kvalifikatsiooniga inimese väljaõpe ning kaasnevad kulud, mis toob kaasa järelevalvetasu kasvu, ei pruugi olla proportsionaalsed järelevalve mahule (vaid neli audiitorettevõtjat on suuremad kui mikroettevõtted).

Mõju RIA-le: *[palume sisendit]*

Mõju Eesti Pangale: *[palume sisendit]*

VIII peatükk. Asjakohaste delegeeritud määruste muutmine

Delegeeritud aktid, ülevaatusklausel, muudatused muudes õigusaktides ja jõustumisaeg (artiklid 50-56) ning kaasnev direktiiv.

Lisaks DORA määrusega kaasneva direktiiviga ettenähtud muudatustele EL direktiivides[10] nähakse eelviidatud artiklites täiendavalt ette ka EL määruste (EC) 2016/2009 (CRA), (EL) 648/2012 (EMIR), (EL) 600/2014 (MiFIR) ja (EL) 909/2014 (CSDR). Muudatused on vajalikud, et viia EL õigusaktid kooskõlla MiCA ja DORA regulatsioonidega.

Mõju Eestile: *Kavandatavad muudatused on vajalikud, et viia DORA määrusega sätestatu kookõlla olemasolevate EL õigusaktidega. Õigusselguse tagamisel on positiivne mõju. Kuivõrd muuta tuleb ka mitmeid direktiive, siis tuleb koostada ka asjaomane seaduse eelnõu. Eesti õiguse vastavusse viimiseks määruse nõuetega, tuleb riigisisest õigust muuta, võimalik, et küberturvalisuse seadust ja finantsinspektsiooni seadust.*

3 EESTI SEISUKOHAD

3.1. Seisukohad digirahanduse paketi kohta üldiselt

Toetame digirahanduse paketi üldiseid eesmärke i) vähendada fragmenteeritust digitaalsel siseturul, (ii) kohandada EL õigus digiajastule vastavaks ja (iii) tõhustada andmete efektiivsemat kasutamist konkurentsieeliste loomiseks.

3.2. Seisukohad digirahanduse strateegia kohta

1. **Toetame digirahanduse strateegia üldisi eesmärke muuta Euroopa finantsteenused digisõbralikumaks ning edendada vastutustundlikku innovatsiooni ja konkurentsi ELi finantsteenuste osutajate vahel.**
   Selgitus: Eesmärkide saavutamiseks võetavate meetmete rakendamine vähendab digitaalse ühtse turu killustatust, et tarbijatel oleks piiriüleselt juurdepääs finantstoodetele ning et finantstehnoloogia idufirmad saaksid oma tegevust laiendada ja kasvada. Sellega tagatakse omakorda, et ELi finantsteenuste eeskirjad vastavad digiajastu nõuetele, näiteks selliste rakenduste puhul nagu tehisintellekt ja plokiahel.
   Euroopa Liidus tuleb tagada, et kehtestatud eeskirjad on ajakohased ja maandavad riske, mis tulenevad uute tehnoloogiate kasutuselevõtust, nt tehisintellekt või plokiahel. Majandus- ja Kommunikatsiooniministeeriumi hinnangul tunduvad strateegias välja toodud ideed toetavat ka meie *fintech startup*ide tegevusi.

[10] 2006/43/EC (raamatupidamise aruanded), 2009/65/EC (UCITS, eurofondid), 2009/138/EU (Solvency II, edasikindlustus), 2011/61/EU (AIFMD, alternatiivsed investeerimisfondid), EU/2013/36 (CRD, kapitalinõuded), 2014/65/EU (MIFID2, finantsinstrumendid), (EU) 2015/2366 (PSD2, makseteenused) and EU/2016/2341 (IORPs, tööandjapension).

2. **Oleme arvamusel, et andmete jagamine on oluline, kuid samal ajal tuleb tagada privaatsuse ja andmekaitse standarditest kinnipidamine ja isikute andmete kaitse.**
   Selgitus: Andmed on uus kuld ja need võimaldavad pakkuda ettevõtjatel väga erinevaid teenuseid ja uuenduslikke lahendusi, mis muudab varasemad protsessid efektiivsemaks. Samas tuleb tagada, et andmetöötlus vastaks kõigile kehtestatud nõuetele ja ei riivaks isikute õigusi. Käesoleval ajal esineb risk, et globaalsed digi-hiiud kasutavad uusi tehnoloogilisi lahendusi, nt tehisintellekti võimalusi, ja EL elanike andmeid tulu teenimise eesmärgil selliselt, mis ei pruugi olla kooskõlas EL nõuetega, eeskätt EL andmekaitset reguleerivate õigusaktidega. Peame tagama, et meil on parem ülevaade selliste ettevõtjate tegevusest ja arvestatavad võimalused rikkumiste korral sekkuda.

3. **Toetame asjakohaseid ja proportsionaalseid meetmeid finantsteenuste kasutajate registreerimise eeskirjade ühtlustamiseks ning digitaalse identiteedi koostalitlusvõime piiriülese raamistiku tõhustamiseks. Seejuures on oluline, et liikmesriikidel oleks võimalik ka edaspidi kasutada loodud usaldusväärseid identimisvahendeid, nt Eestis e-ID, mobiil-ID, Smart-ID.**
   Selgitus: Euroopa 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 koostalitlusvõime piiriülest raamistikku. Teema on Euroopa Komisjoni jaoks prioriteetne.
   Toetame Euroopa Komisjoni eesmärke AML/CFT vallas ja e-IDAS regulatsiooni ülevaatamise osas. E-IDASe osas on oluline, 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 oleme seisukohal, 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.

4. **Toetame andmepõhise innovatsiooni edendamine rahanduses ühise finantsandmeruumi loomise kaudu.**
   Selgitus: 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.“* Viidatud dokumendi leheküljel 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, muuhulgas seetõttu, et 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.

5. **Toetame EL õigusaktide ülevaatamise ja muutmise, et tagada avalikustatud teabe kättesaadavus standardses ja masinloetavas vormingus. Peame oluliseks, et EL õigusaktide ülevaatamise käigus kõrvaldatakse ka innovatsiooni pärssivad võimalikud olulised regulatiivsed tõkked.**
   Selgitus: Toetame 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.
Seadusandlus tuleb kaasajastada, et vältida innovatsiooni pärssimist, mida tekitavad pärand-normid, mis ei vasta kaasaja vajadustele ja ei ole enam asjakohased.

6. **Toetame ELi digirahanduse platvormi loomist, et edendada koostööd era- ja avaliku sektori sidusrühmade vahel.**
Selgitus: EL on kavandamas digirahanduse platvormi loomist, mis toob kokku uuenduslikud tehnoloogilised algatused, võimaldab koostööd järelevalvega ja pakub ka rahalisi toetusmeetmeid äriidee rakendamiseks.
Euroopa Komisjon on selgitanud, et: *Era- ja avaliku sektori sidusrühmade koostöö soodustamiseks loob komisjon koostöös EFIFiga*[11] *uue ELi digirahanduse platvormi. Uus platvorm toimib uue digirahanduse ökosüsteemiga internetis pideva suhtlemise kanalina, tuginedes digirahanduse valdkonna teabevahetuse raames saadud positiivsele tagasisidele. Samuti annab see liidese EFIFile ning riiklikele innovatsioonisoodustajatele ja riiklikele e-litsentside andmise menetlustele. Edaspidi võib selle kujundada laiemaks koostööplatvormiks ja andmeruumiks, mida sektor või järelevalveasutused saavad kasutada innovaatiliste lahenduste katsetamiseks. Platvorm töötatakse välja nii, et seda oleks võimalik rahastada programmist „Digitaalne Euroopa", mis toetab digitehnoloogia süvalaiendamise koostööplatvormide kasutuselevõttu.*[12]

3.3. Seisukohad uuendatud jaemaksete strateegia kohta

1. **Toetame jaemaksete strateegias Euroopa üleselt seatud üldiseid eesmärke.**
Selgitus: *Toetame Euroopa üleselt seatud eesmärke ja oleme valmis neid rakendama, kuid saame täpsema seisukoha esitada tulenevalt konkreetsetest regulatiivsetest ettepanekutest.*

2. **Toetame SEPA välkmaksete võimalikult laiaulatuslikku, euroopaülest kasutuselevõttu.**
***Selgitus*:** Eestis on välkmaksete osakaal 61% pankadevahelistest maksetest (sept 2020). Välkmaksete makseskeemiga on liitunud 6 turuosalist (4 suurpanka, TBB ja Pocopay).. 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 välkmakseteskeemi kasutusele võtnud.
Et saavutada välkmakselahenduste koostoimimine ja piiriülene kasutamine võib olla vajalik ühtlustatud lähenemine EL-tasandil ja skeemide standardiseerimine. Toetame Euroopa Komisjoni nägemust muuta välkmaksed nn. uueks normaalsuseks. Tagasinõude õiguse laiendamine välkmaksetele, on küsitav, sest välkmaksed on kreeditkorraldused, millele ei rakendata tagasinõudeõigust. Sarnase tagasinõude kehtestamine välkmaksete suhtes nagu SEPA otsekorralduste puhul tooks kaupmeestele ja ka eraisikutele kaasa ebakindluse ootamatute makse tagasinõuete näol. Sellist negatiivset mõju tuleks vältida. Tagasinõude esitamise asemel ja välkmaksete turvalisuse tõstmiseks saame toetada üleeuroopalise makse saaja nime ja kontonumbri kontrolli lahenduse loomist ning kasutamist enne makse kinnitamist.
Toetame algatust, mis näeb ette välkmaksete süsteemide omavahelise liidestamise (teiste maksesüsteemidega). Vastava algatuse idee seisneb erinevate süsteemide koostoimivuses, tarbijate rahulolu suurendamises ning üleeuroopalise välkmaksete ulatuse saavutamises. Samuti saame toetada kolmandate riikide liitumist maksesüsteemidega TIPSi või RT1, kui süsteemi hoolsusnõuded on täidetud ning rahapesu tõkestamise ja terrorismi rahastamise riskid on adekvaatselt maandatud.

[11] Euroopa innovatsioonisoodustajate foorum
[12] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2020:0591:FIN:ET:PDF, lk 8.

3. **Toetame Euroopa Komisjoni tegevusi, mille eesmärgiks on kaupmeeste, eelkõige väikeettevõtjatele suunatud makselahenduste täiustamine ja lihtsustaminening erinevate makselahenduste kohta teadlikkuse suurendamine. Lisaks toetame makseahela täielikku digitaliseerimist, sh üleeuroopalise e-arve request-to-pay) ja e-kviitungi väljaarendamist ja kasutuselevõttu.**
***Selgitus*:** Toetame Euroopa Komisjoni eelloetletud tegevussuundasid sh kaupmeeste, eelkõige väikeettevõtjate makselahenduste täiustamist ja lihtsustamist ning nende teadlikkuse suurendamist erinevatest maksevõimalustest ja - lahendustest. Toetame 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.
Eesti Pank viis 2020. aasta suvel väikeettevõtjate seas läbi küsitluse, mille eesmärk oli saada teada, kas ettevõtjad on huvitatud makselahendusest, mis võimaldavadneil oma toodete või teenuste eest tasumisel kasutada pangaäppi või QR-koodi ning saada tasu välkmaksena. Uuringust selgus, et väikekaupmehed on huvitatudmakselahendustest, mis ei põhine kaardimaksetaristul. 76% vastanutest tõid välja, et tunnevad uue makselahenduse vastu huvi, kui see oleks soodne, tarbijale mugav ja tagaks raha kiirema laekumise.
Maksekeskkonna arendamise küsimusi arutab Eesti Pank regulaarselt koostöös turuosalistega. Digitaliseerimise ja uuendamise eesmärgil on äsja Maksekeskkonna Foorumi alla loodud maksekeskkonna digitaliseerimise töögrupp.

4. **Toetame siseriiklike eID ja eAllkirja lahenduste üleeuroopalist tunnustamist ja kasutamist finantssektoris ning eIDAS asjakohastamist.**
***Selgitus*:** Toetame 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 piiriüleselt e-idenditeete ja eAllkirju, mitte uue „Euroopa lahenduse“ loomist. Seega saame toetada koostalitlust võimaldavat süsteemi, et kasutatada olemasolevaid ID-kaardi, Mobiili-ID kui ka Smart-ID lahendusi kõikjal Euroopas.

5. **Toetame eletrooniliste maksete ja sularaha kasutamise ning kättesaadavuse uuringu läbiviimist.**
***Selgitus*:** Toetame 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.
Toetame algatusi, mis on suunatud euro sularaha kättesaadavuse tagamiseks ning kindlustavad, et euro pangatähed ja mündid on tarbijate ja kaupmeeste poolt aktsepteeritud maksevahendiks. Toetame maksekeskkonda, kus saab kasutada erinevaid makseviise ning oleks tagatud ühiskonnas alternatiivne lahendus, kui üks või teine maksesüsteem ei peaks töötama. Enne konkreetsete meetmete kasutusele võtmist pooldame põhjaliku analüüsi koostamist eesmärgiga selgitada välja sularaha vastuvõetavust ning kättesaadavust piiravad tegurid, et kavandatavad meetmed oleksid võimalikult mõjusad.

6. **Toetame avatud panganduse põhimõtte ja makseteenuste turvalisust tugevdavate meetmete rakendamist ning Euroopa Komisjoni poolseid samme meetmete rakendamise hindamiseks.**
***Selgitus*:** Toetame avatud panganduse põhimõtete ja maksekeskkonna turvalisust tagavate meetmete juurutamist. Seda aitavad tagada muu hulgas maksekontode juurdepääsuliideste (API) üleeuroopalise standardi ja ühetaolise rakendamise skeemi (reeglistiku) väljatöötamine. Eestis on võimalik kasutada avatud pangandusel põhinevaid teenuseid – nii kontoteabe kui ka makse algatamise teenust. Kontoteabe teenuse

puhul on võimalik teenusega siduda mitut maksekontot. Makse algatamise teenuse näiteks on universaalne pangalink.

Toetame makseteenuste turvalisust tugevdavate meetmete rakendamist ning Euroopa Komisjoni poolseid samme meetmete rakendamise jälgimiseks.

Toetame tugeva autentimise nõude rakendamist üleeuroopaliselt. 31. detsembril 2020 jõustub kaarditehingutele tugeva autentimise nõue ning kõikide e-poodide kaardimakselahendused peavad toetama tugeva autentimise võimalust.

Toetame Euroopa Komisjoni poolset analüüsi maksete turvalisuse küsimuses, et vähendada maksepettuseid. Selle raames uuritakse muu hulgas, kas maksekonto omaniku nime ja maksekonto numbri (IBANi) kokkulangevuse kontroll aitab kaasa pettuste vähendamisele ning mil määral saaks viipemakse summat suurendada, et see ei tooks kaasa täiendavaid riske.

Et makseteenusepakkujad oleksid võimelised end küberrünnakute eest kaitsma, toetame Euroopa Komisjoni eelnõu DORA vastuvõtmist ning sidumist eurosüsteemi küberkerksuse testiraamistikuga TIBER-EU. Lisaks analüüsime Eesti finantssektorile TIBER raamistiku pakkumise vajadust.

7. **Toetame Euroopa Komisjoni algatust anda maksesüsteemidele otsesenet juurdepääs e-raha asutustele ja makseasutustele.**

***Selgitus*:** Toetame Euroopa Komisjoni soovi laiendada maksesüsteemides osalemise skoopi, tagades juurdepääsu maksesüsteemidele ka e-raha asutustele ja makseasutustele. Maksesüsteemidele juurdepääsu võimaluse loomine ka teistele makseteenuse pakkujatele kui pangad, annab võimaluse kohelda turuosalisi võrdselt ning kasvataks arveldusturul konkurentsi, millest võidaksid lõpptarbijad. Täiendavate õiguste andmisel tuleb tuvastada ja katta osalemisega kaasnevad (e-raha asutuste ja makseasutuste) kõikvõimalikud riskid ning tagada nende riskide maandamine süsteemioperaatorite poolt kooskõlas süsteemi suhtes kehtestatud järelevaatamise nõuetega.

8. **Toetame Euroopa Komisjoni kavatsust analüüsida, kuidas tagatakse juurdepääs makseteenuste osutamiseks vajalikule tehnilisele taristule ja kas võimalikud takistused selles on õiguspärased..**

***Selgitus*:** Toetame Euroopa Komisjoni ettepanekut viia läbi analüüs, kuidas on tagatud juurdepääs makseteenuste osutamiseks vajalikule tehnilisele infrastruktuurile (nt funktsionaalsus, mis võimaldab andmevahetust kahe lähikontaktis oleva seadme vahel, nn mobiilseadmete NFC). Üheks kõnealuseks näiteks on Apple'i seadmed, mis piiravad NFC funktsionaalsuse kasutamist muudele kui Apple lepingulisetele partneritele. See tähendab, et Apple soovib saada tasustatud iga makse pealt, mis sooritakse Apple seadmega.

3.4. Seisukohad krüptovarade seadusandliku ettepaneku kohta (MiCA määrus ja selle lisad)

1. **Toetame üldiselt Euroopa Komisjoni uue Euroopa Liidu õigusraamistiku väljatöötamist krüptovarade, sealhulgas varaga tagatud krüptovarade (*asset-backed tokens*), e-raha tokenite (*e-money tokens*), ja kasutustokenite (*utility tokens*) osas ning eelnimetatud krüptovaradega seotud teenuseosutajate osas.**

Selgitus: Teatavad tehnoloogia hiiud on andud avalikkusele sõnumeid, et nad kavatsevad Euroopa turule tuua tagatud krüptovaral põhinevaid makselahendusi (sh Libra), mida praegusel hetkel on keeruline kindlasse regulatsiooni paigutada. Selleks, et säiliksid tarbijate kaitseks seatud tingimused ning aus konkurents Euroopa makseturul, peavad makselahendused (sh uudsetel tehnoloogiatel põhinevad väärtuse ülekandmise võimalused) olema kooskõlas kehtiva õigusraamistikuga ning ka õigusraamistiku peab vajadusel kohandama selliseks, mis arvestaks tehnoloogiliste arengutega. Ühtlasi aitaks selgesõnaline regulatsioon tehnoloogiat edasi aren-dada ja seeläbi toetada innovatsiooni; samuti leida EL-ile koht digitaalse rahanduse maailmas.

2. **Toetame Komisjoni poolt võetud lähenemist reguleerida kõiki krüptovarade liike, kuid teha seda proportsionaalsel moel, arvestades vastava krüptovaraga kaasnevat riski investoritele kui Liidu finantsstabiilsusele tervikuna.**
Selgitus: Määruse ettepanekus on reguleeritud eraldi kolme tüüpi krüptovara – kasutustokenid, varaga tagatud tokenid ja e-raha tokenid. Nimetatud eri tüüpi krüptovaradele on sätestatud ka erinevad nõuded lähtuvalt nendega seotud riskidest, kuid ka eeldatavast kasutuselevõtu ulatusest ning pakkumise mahust – näiteks kasutustokenitele (mille peamine funktsioon on olla vahetatav ligipääsu eest mõnele digitaalsele tootele või teenusele) on kehtestatud peamise pakkumise läbiviimise nõudena ainult põhiteabedokumendi avalikustamise ja finantsjärelevalveasutusele teadmiseks esitamise kohustus, kuivõrd kasutustokenitega seotud riskid on üsna piiratud ühe pakkumisena, ning põhiteabedokument on minimaalne nõue, mille täitmine võimaldab investoril teha informeeritud otsuse krüptovara omandamise kohta. Seevastu varaga tagatud tokenite ja e-raha tokenite emitentidel on vajalik enne pakkumist kooskõlastada põhiteabedokumendi sisu finantsjärelevalveasutusega, ning taotleda tegevusluba, mis tähendab seda, et enne pakkumise alustamist toimub krüptovarade pakkuja enda sisuline hindamine nii tema organisatoorsete nõuete kui sisemiste protsesside toimimise osas. Samuti peab nimetatud tokenite pakkujatel olema olemas omavahendid, millega tagatakse tokenihoidjate nõuded emitendi vastu. Nimetatud rangemad nõuded on vajalikud, kuivõrd selliseid tokeneid emiteeritakse tavaliselt suuremas mahus ning need on kasutusel väärtuste ülekandmiseks (st makseteks).

3. **Eelistame, et määruse kohaldamisalas oleksid ka sellised krüptovarad, mis kannavad endas investeerimisriski, ning mis oleksid pigem väärtpaberi-tüüpi krüptovarad (kuid mitte vabalt võõrandatavad väärtpaberid MiFID mõistes).**
Selgitus. Kehtiv EL õigus ei reguleeri selliseid instrumente, mis oma funktsioonilt sarnanevad väärtpaberiga, kuid ei ole väärtpaberid MiFID mõistes (st mitmepoolses kauplemiskohas kaubeldavad väärtpaberid ehk aktsiad, võlakirjad, jne). Nimetatud määratluse alla võiksid minna näiteks osaühingute osad, mille käitlemine on siseriiklikult reguleeritud. See aga põhjustab õiguse killustatust liikmesriikide vahel. Lisaks kujutab see meie hinnangul suuremat investeerimisriski, kui nn kasutustokenid, mis määruse reguleerimisalasse kuuluvad.

4. **Peame oluliseks, et Komisjon selgitaks delegeeritud aktis või juhendites, et kuidas eristada e-raha tokenit ja varaga tagatud tokenit piiripealsete juhtumite puhul. Lisaks ei ole me jätkuvalt veendunud kahe varaga tagatud tokeni kohta eraldi režiimi vajalikkuses.**
Selgitus. Praktikas võib olla nimetatud instrumentide vahetegu kohati keeruline. Kuivõrd e-raha tokeni näol on tegemist ühe varaga tagatud tokeni eriliigiga, mis on tagatud ainult ühe riikliku valuutaga, ning millele rakenduvad rangemad nõuded võrreldes varaga tagatud tokenitega, siis on oluline teha vahet nendel kahel instrumendil. Vastavates EL töögruppides on juhitud tähelepanu näiteks võimalusele, et token võib olla tagatud euroga 99% ulatuses ning 1% ulatuses muu valuutaga, mis teeks sellest varaga tagatud tokeni, kuigi majanduslikus mõttes on ilmselt tegemist siiski e-raha tokeniga. Vähem äärmuslikum erand oleks selline krüptovara, mille väärtus on proportsionaalselt tagatud euroalal kasutusel olevate valuutade suhestumusega kogu EL-i SKT-sse (ehk 80%+ euro, aga vähesel määral tagatud rootsi krooniga, poola zlotiga, tšehhi krooniga jne).

5. **Eelistame, et olemasolevad turuosalised (st pangad) peaksid varapõhiste tokenite või e-raha tokenite emiteerimisele eelnevalt kas taotlema eraldi tegevusloa või registreerima sellekohase tegevuse finantsjärelevalveasutuse juures; viimasel juhul näidates, et neil on olemas vajalikud teadmised, oskused ja süsteemid nimetatud tegevuste ja teenuste osutamiseks.**
Selgitus. Ettepaneku teksti kohaselt võivad pangad pakkuda avalikkusele varaga tagatud tokeneid ja e-raha tokeneid ilma täiendava tegevusloa või registreerimiskohustuseta; ainus märkimisväärne kohustus on avalikustada nimetatud tokeni kohta käiv põhiteabedokument. Oleme seisukohal, et panga keskne tegevus pangandusdirektiivi alusel ei peaks hõlmama e-raha tokenite või varaga tagatud tokenite väljastamist,

kuivõrd sellise tegevusega kaasnevad süsteemsed riskid ning nimetatud tegevus ei peaks olema lubatud ainult olemasoleva panga tegevusloa alusel.

6. **Märgime, et määruse kavand sisaldab mitmeid viiteid EBA ja ESMA poolt loodavatele tulevastele standarditele selles osas, mis puudutab krüptovarateenuste osutamisele seatud nõudeid. Peame oluliseks, et sisulised nõuded teenuseosutajatele tuleneksid eelkõige õigusaktist, mitte ei selguks näiteks aasta pärast määruse vastuvõtmist.**
Selgitus. Toetame võimalikult laiaulatuslikku reguleerimist pigem määruse tekstis kui määruse alusel antud aktides; vastasel juhul võib olla juba välja kujunenud turuosaliste seas praktika ja standardid, mida tuleks vastavalt hiljem kehtestatud nõuetele muuta.

7. **Toetame üldiselt määruse kavandi lisas toodud nõudeid põhiteabedokumendile, kuid nimetatud nõuded võivad vaja kohati täpsustamist.**
Selgitus. Üldiselt on nõuded sobivad ja kohased pakutavatele instrumentidele, kuid eelnimetatud nõudeid võib olla vajalik täpsustada eeskätt investoritele kaasnevate riskide osas. Samuti oleks vajalik selgelt krüptovarade pakkuja poolt asjakohasel juhul (st kasutustokenite emiteerimisel) kommunikeerida, et finantsjärelevalveasutus ei ole enne pakkumise algust heaks kiitnud põhiteabedokumendi sisu.

3.5. Seisukohad hajutusraamatu tehnoloogial põhineva turuinfrastruktuuride katserežiimi kohta

1. **Toetame üldiselt Euroopa Komisjoni tahet töötada välja uus Euroopa Liidu režiim, mis lubab taotleda erandit väärtpaberite pakkumise ja registreerimisega seotud õiguslikest raamistikest ning mis peaks soodustama innovatsiooni ja konkurentsi selles vallas.**
Selgitus: Hajusraamatusüsteemide kasutamine on kehtiva EL õiguse alusel väga piiratud – eeskätt kasutatakse hajusraamatusüsteeme kasutustokenite ja maksetokenite jaoks. Seevastu kehtiv õiguslik raamistik (MiFID II, CSDR) ei toeta hajusraamatusüsteemidel peetavate väärtpaberite kasutuselevõttu, ning väärtpaberite kauplemiskohad ja keskdepositooriumid suuresti selles sektoris ei osale. See on aga viinud arengu pidurdumiseni ja õiguse killustumiseni selles vallas (kuivõrd EL üleselt ei ole ühest režiimi hajusraamatusüsteemil põhinevate väärtpaberite pakkumiseks, registreerimiseks ja kauplemiseks). Põhjendatud alustel erandi taotlemine kahe eeltoodud EL õigusakti sätetest peaks andma pilootprojekti toimimise käigus paremat selgust selles osas, kas ja mil määral takistavad olemasolevad õigusaktid innovatsiooni edendamist hajusraamatusüsteemides peetavate väärtpaberitega seotud ärimudelites.

2. **Toetame üldiselt määruse kavandis esitatud sätteid, mis puudutavad kohaldamisala, taotletavate erandite ulatust ja määruse (esialgset) kehtivustähtaega.**
Selgitus: Seoses määruse kavandis toodud kohaldamisalaga (st et ainult investeerimisühingud ja krediidiasutused saavad taotleda erandit MiFID-ist ja CSDR-ist) märgime, et väärtpaberite pakkumise, registreerimise ja kauplemise sektor on riskantne, mistõttu on EL tasandil ette nähtud mitmed turvameetmed ja hoolsusnõuded, mida tuleb täita enne, kui teenuseosutaja saab finantsjärele-valveasutuselt loa nimetatud teenuseid osutada. Kuigi kõrgemate hoolsusmeetmete rakendamine on vajalik eriti niivõrd uudses teenuste valdkonnas nagu kõnesolevate väärtpaberitega seotud teenused, siis on meil tekkinud murekoht, et teenustele ligipääsu künnised on seatud niivõrd kõrgeks, et see ei ajenda uuemaid ja väiksemaid ettevõtjaid sektoris osalema. Lisaks vajaks Komisjoni poolt selgitamist, et kas näiteks investeerimisühingu tegevusloa andmise eeldustest on võimalik kõrvale kalduda, kui ettevõtja soovib osutada registripidamise teenust, kuid mitte MiFID väärtpaberite jaoks.

3.6. Seisukohad digitaalse operatsioonilise vastupidavuse ehk finantsteenuste tegevuskerksuse seadusandliku ettepaneku kohta (määrus ja direktiiv)

1. **Peame oluliseks ennetada ja maandada finantssektoris esinevaid digitaalseid riske, sh küberriske, mis on tingitud järjest suuremast sõltuvusest tarkvarast ja digitaalsetest protsessidest ja mis ühtlasi tähendab ka info- ja kommunikatsioonitehnoloogiaga seotud riskide tõusu. Seetõttu toetame sektori-spetsiifiliste ühetaoliste nõuete kehtestamist IKT süsteemide turvalisusele, tagades kõrgtasemelise digitaalse operatsioonilise vastupidavuse.**
   Selgitus: Et finantssektor suudaks vastu pidada igasugust tüüpi IKT-ga seotud häiretele ja ohtudele, kehtestatakse kavandatava määrusega ühtsed nõuded finantsteenuste digitaalse operatsioonilise vastupidavuse kohta ehk sektori-spetsiifilised ühetaolised nõuded IKT süsteemide turvalisusele, hõlmates ka riskijuhtimist, intsidentidest raporteerimist, vastupidavusvõime testimist ja infojagamist. NIS direktiiv ei hõlma kogu finantssektorit ja seetõttu ei kohaldu ka küberturvalisuse seadus kõikidele finantsteenuste osutajatele. Lähtuvalt eelnevast toetame sektorispetsiifilise õigusraamistiku loomist, mis ühtlustab nõudeid sektoris ja muudab finantsökosüsteemi vastupidavamaks digitaalsetele ohtudele.
   Määrusega kehtestatavad nõuded on käesoleval ajal kaetud erinevate standardite ja seadustega. Näiteks ISO27000 perekonna standardid, suuremahulistest intsidentidest teavitamist reguleerib täna küberturvalisuse seadus, hädaolukorra seadus ja Finantsinspektsiooni juhendid (nt nõuded finantsjärelevalve subjekti infotehnoloogia ja infoturbe korraldusele), 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 leiame, et kogu sektorile ühtlustatud baasnõuete kehtestamine määruse näol on pigem positiivne ja selgust loov eesmärk. Oluline on järgida proportsionaalsuse põhimõtteid.

2. **Leiame, et määruse kohaldamisalas võiksid olla hõlmatud enamik finantssektori osalisi, eeskätt olulised turutegijad.**
   Selgitus: Eelistame, et kohaldamisalasse oleksid hõlmatud kõik finantsteenuste osutajad, sealhulgas ka maksesüsteemid. Kuivõrd ettepanek on reguleerida finantssektori IKT riskide maandamise meetmed, siis ei ole meie hinnangul maksesüsteemide välistamine õigustatud. Eeskätt, kuna maksesüsteemid ei ole hõlmatud ka NIS direktiiviga ja seetõttu ei laiene käesoleval ajal neile ka küberturvalisuse seaduse nõuded. Maksesüsteemid on oluline osa finantssektorist ja tuleks seetõttu DORA skoopi hõlmata. Maksesüsteemid on järelevaadatavad keskpankade poolt ja allutatud keskpanga sätestatud riskide maandamise nõuetele. Kindlasti tuleb vältida dubleerivaid nõudeid. Riigi siseselt koostöö pädevate asutuste vahel (Finantsinspektsioon, RIA, Eesti Pank) aitaks kindlasti dubleerimist vältida. Eesti vaatest ei oleks maksesüsteemide välistamine vajalik.

3. **Toetame proportsionaalsusnõuete ülevaatamist, hindamaks kas määrusega pakutud leevendused on mikroettevõtjatele piisavad.**
   Selgitus: Määrus põhineb proportsionaalsuse printsiibil, pakkudes leevendusi mikroettevõtjatele. Käesoleval ajal puudub analüüs selle kohta, kas pakutud meetmed on piisavad, et määrusest tulenevad nõuded ei muutuks mikroettevõtjatele liigselt koormavaks. Samas nendime, et küberkurjategijad otsivad pidevalt nõrku kohti ja ka mikroettevõtjatel peaksid olema paigas proportsionaalsed meetmed, mis aitaksid toime tulla digitaalsete ohtudega. Kuivõrd kõnealune teema ei ole käesoleval ajal selge, siis eelistame, et mikroettevõtjatest audiitorid võiksid olla regulatsiooni skoobist väljas. Seega tuleb kaaluda, kas näiteks kindlustusagentide ja -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.

4. **Toetame testimisnõuete kehtestamist, kuna DORA määruse näol on kogu finantssektorile ühtlustatud baasnõuete kehtestamisel selgust loov eesmärk. Samas peaks DORA andma finantssektori kriitiliste**

infrastruktuuride küberkerksuse testimise osas selgeid viiteid ja seoseid eurosüsteemiülesele küberkerksuse testiraamistikule TIBER-EU.

Selgitus: 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. Leiame, et DORA määrus peaks finantssektori kriitiliste infrastruktuuride küberkerksuse testimise osas andma selgeid viiteid ja seoseid eurosüsteemiülesele küberkerksuse testiraamistikule TIBER-EU, mis aitaks harmoniseerida kübertestide tegemise üle Euroopa ning annaks pädevatele asutustele võimaluse testitulemusi valideerida.

Määruse kohaselt tuleb finantssektori ettevõtete küberkerksuse testid kooskõlastada ja valideerida pädeva asutuse poolt, mis on positiivne nähtus. Eesti Tiber-EU raamistiku rakendamise vajaduse väljaselgitamiseks on vajalik kahtlemata pidada dialoogi Eesti finantssektori turuosalistega. Eesti Pangaliit on teada andnud, et toetab Tiber-EU raamistiku implementeerimist. 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.

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.

5. **Toetame asjakohaseid ja proportsionaalseid meetmeid IKT riskide juhtimisele ja viidatud riskidega seotud juhtumite halduse, klassifitseerimise ja raporteerimise kohta.**

   Selgitus: DORA

   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 ja vähendaks halduskoormust. 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.

   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.

   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 nähtus.

6. **Toetame asjakohaseid ja proportsionaalseid meetmeid kolmandate osapooltega seotud IKT riskide juhtimise kohta.**

   Selgitus: Leiame, et määrusega kavandatavad meetmed, mille eesmärk on maandada kolmandatest osapooltest IKT teenuse osutajatega seotud riske, on mõistlikud. Määrusega kehtestatakse nt põhimõtted, mida tuleb arvesse võtta teenuste sisseostmise puhul, nt lepingut sõlmides. See peaks andma finantsteenuste osutajatele võrdsemad alused läbirääkimise protsessis.

7. **Leiame, et järelevalve kolmandatest osapooltest kriitiliste IKT teenuseosutajate üle on vajalik.**

   Selgitus: Üldiselt nõustume, et kriitilise tähtsusega IKT teenuseosutaja üle tuleks teostada järelevalvet ja see võib olla mõjusam juhituna keskselt EL tasandil. Käesoleval ajal ei ole veel selge ja tuleb kindlasti täpsustada,

kes on kriitiline teenuseosutaja, kuidas toimub juhtiva järelevalveasustuse vahetumine tulenevalt tema määratlemise tingimustele vastavuse muutumisest pidevalt/jooksvalt ning kuidas toimub järelevalve kriitilise tähtsusega IKT teenuseosutajate üle kooskõlas NIS direktiiviga.
NIS direktiiv on horisontaalne õigusakt, mis reguleerib võrgu- ja infosüsteemide turvalisust. See on Eestis üle võetud küberturvalisuse seadusesse. Viidatud õigusakt kohaldub IKT teenuseosutajatele, täiendavad nõuded (EL tasandil järelevaatamine) lisanduvad DORA määrusest sellisele isikule üksnes siis, kui tegemist on kriitilise IKT teenusepakkujaga, kes osutab teenuseid ka finantssektorile. Kriitilisus on sisustatud DORA määruse artikli 28 lõikes 2. Käesoleval ajal ei ole teada, kas Eestis sellistele kriteeriumitele vastavat teenuseosutajat üldse on.

8. **Oleme arvamusel, et riigisiseste pädevate asutuste nimetamine ja rollijaotus peaks jääma liikmesriikide otsustada.**
Selgitus: Määruse reguleerimisalasse kuuluvate tegevusvaldkondade ja artiklis 44 nimetatud pädevate asutuste regulatsioon tuleks kujundada selliselt, kus Eestis vastav roll kontsentreeritakse. Samas peab olema tagatud võimalus liikmesriikidel ise asjaomaseid pädevusi jaotada vastavalt vajadustele. Näiteks ei oleks mõistlik küberpädevusega hakata sisustama audiitorite järelevalve nõukogu. Vajalik on koostöö pädevate asutuste vahel.

9. **Toetame vabatahtliku infovahetuse puhul seaduslike aluste loomist.**
Selgitus: 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. Juhul kui info jagamine toimub piisavalt üldiselt tasemel ilma tehniliste detailideta, siis ei tohiks teavitamisega kaasneda ülemäära suuri ohtusid ega takistusi.
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. Seega toetame finantssektori spetsiifilise infojagamiskeskkonna loomist. Ohte aitavad elimineerida osapoolte vahel sõlmitavad koostöökokkulepped, kus määratletakse info jagamise tingimused.