Finantskriisi ennetamise ja lahendamise seaduse ning teiste seaduste muutmise seaduse eelnõu seletuskiri

1. Sissejuhatus

1.1. Sisukokkuvõte

Eelnõuga tagatakse kooskõla riigisisese finantssektori tegevust reguleeriva õiguse ja finantsasutustele kohalduvate Euroopa Liidu (edaspidi ***EL***) digitaalse tegevuskerksuse nõuete vahel.

Põhieesmärk on vähendada finantssektoris äriprotsesside ja oluliste funktsioonide katkemise riski ning ohtu nii ettevõtte kui ka klientide teabe- ja finantsvarale, mida võivad põhjustada nii tehnilised rikked, operatiivsed vead kui ka küberründed, ning seeläbi suurendada muu hulgas finantsteenuste klientide ja investorite kaitset.

Finantsteenuste valdkonnas toimunud digiüleminek on toonud kaasa info- ja kommunikatsioonitehnoloogia (edaspidi ***IKT***) teenuste kasutamise ja neile tuginemise enneolematul tasemel. Finantsteenuste osutamine ilma pilvteenuseid, tarkvaralahendusi ja andmetega seotud teenuseid kasutamata on muutunud mõeldamatuks. Digitaalse tegevuskerksuse nõuete rakendamise eesmärk on tagada finantsasutuste:

- tegevuse toimimine, terviklikkus ja usaldusväärus mh IKT suutlikkusega seonduvalt;
- võime kohaneda, toimida ja taastuda IKT-ga seotud riskide realiseerumisel, sh küberrünnete korral;
- suutlikkus teenuse osutamist kiiresti jätkata.

Finantsasutustele suunatud EL digitaalse tegevuskerksuse nõuded on sätetatud:

- Euroopa Parlamendi ja nõukogu määruses (EL) 2022/2554[1], mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 (edaspidi ***DORA määrus***) ja
- Euroopa Parlamendi ja nõukogu direktiivis (EL) 2022/2556[2], millega muudetakse direktiive 2009/65/EÜ, 2009/138/EÜ, 2011/61/EL, 2013/36/EL, 2014/59/EL, 2014/65/EL, (EL) 2015/2366 ja (EL) 2016/2341 seoses finantssektori digitaalse tegevuskerksusega (edaspidi ***DORA direktiiv***).

Eelnõuga võetakse üle DORA direktiiv, mille ülevõtmistähtaeg on 17. jaanuaril 2025. a. Ühtlasi tagataks finantssektori seaduste kooskõla DORA määrusega.

Digitaalse tegevuskerksuse nõuete kohaldamisalasse kuuluvad finantsasutused on:

- krediidiasutused;
- hoiu-laenuühistud (riigisisene valik mitte kohaldada määrust);
- makseasutused;
- e-raha asutused;
- investeerimisühingud;
- alternatiivsete investeerimisfondide valitsejad;
- fondivalitsejad;
- aruandlusteenuse osutajad;
- kindlustus- ja edasikindlustusandjad;
- kindlustusvahendajad (v.a kuni keskmise suurusega vahendajad);

[1] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32022R2554
[2] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32022L2556

- krüptovarateenuse osutajad ja varapõhiste tokenite emitendid;
- reitinguagentuurid;
- kriitilise tähtsusega võrdlusaluste haldurid;
- ühisrahastamisteenuse osutajad;
- väärtpaberistamise registrid;
- väärtpaberite keskdepositooriumid;
- kesksed vastaspooled;
- ühisrahastusteenuse osutajad;
- kauplemiskohad;
- kauplemisteabehoidlad ja
- tööandja kogumispensioni asutused (IORP-id).

Finantsasutus peab:
- kehtestama tõhusa ja usaldusväärse IKT-riskide juhtimisraamistiku, mis on dokumenteeritud ja auditeeritud, võimaldades IKT-ga seotud riske kiiresti ja tõhusalt juhtida;
- teavitama pädevat asutust tõsistest IKT intsidentidest;
- testima regulaarselt ettevõtte digitaalset tegevuskerksust;
- jagama (vabatahtlikult) küberohtudega seotud infot teiste finantsasutustega;
- muu hulgas juhtima kolmandast isikust IKT teenuseosutajaga seotud riske, sealhulgas järgima finantsasutuse ja kolmandast isikust IKT teenuseosutaja vahelistele lepingutele kohalduvaid põhimõtteid.

DORA kohaldamisalasse kuuluvad lisaks kriitilise tähtsusega kolmandast osapoolest IKT teenuseosutajad, kelle suhtes kohaldub EL-ülene järelevaatamisraamistik.

Seega mõjutab uus regulatsioon kõiki finantsasutusi, kelle halduskoormus küll tõuseb, kuid hästi toimiv IKT-riskide juhtimisraamistik ja digitaalse tegevuskerksuse testimine aitab ennetada IKT-ga seotud riskide realiseerumist, samas riskide realiseerumisel aitab tagada, et ettevõte saab kiiresti jätkata oluliste funktsioonide osutamist. Kui finantsasutusel on toimiv IKT riskide juhtimisraamistik, on ka klientidega seotud teabe- ja finantsvara paremini kaitstud ning lisaks on klientidele teenuse osutamise katkemise risk oluliselt väiksem.

Lisaks tehakse tehnilised muudatused, et viia finantssektori seadused kooskõlla äriseadustikus (ÄS) 2022. aasta 23. detsembril ja 2023. aasta 1. veebruaril jõustunud muudatustega. Sellega eemaldatakse seadustest tühi viide ning lisatakse vastav regulatsioon seaduste teksti ning ajakohastatakse ühinguõigust reguleerivaid sätteid.

Eelnõuga tehtavad muudatused jõustuvad osaliselt üldkorras ning DORA määruse ja direktiivi nõuete rakendamisega seotud sätted 17. jaanuaril 2025. a.

1.2. Eelnõu ettevalmistaja

Eelnõu ja seletuskirja on välja töötanud Rahandusministeeriumi finantsteenuste poliitika osakonna nõunik Kristiina Kubja (58851398, Kristiina.Kubja@fin.ee), sama osakonna osakonnajuhataja Siiri Tõniste (58851466, Siiri.Toniste@fin.ee) ja osakonnajuhataja asetäitja Thomas Auväärt (6113633, Thomas.Auvaart@fin.ee). Eelnõu väljatöötamisel konsulteeriti Finantsinspektsiooni (FI), Riigi Infosüsteemide Ameti (RIA), Eesti Panga (EP), Majandus ja kommunikatsiooniministeeriumi (MKM) ja Riigikantseleiga (RK).

Eelnõu ja seletuskirja juriidilist kvaliteeti kontrollis Rahandusministeeriumi personali- ja õigusosakonna nõunik Marge Kaskpeit (58851423, Marge.Kaskpeit@fin.ee) ja keeleliselt toimetas sama osakonna keeletoimetaja Sirje Lilover (58851468, Sirje.Lilover@fin.ee).

1.3. Märkused

Eelnõu on seotud Vabariigi Valitsuse tegevusprogrammi punktiga 2.1.3, mille kohaselt tuleb finantskriisi ennetamise ja lahendamise seaduse eelnõu direktiivi (EL) 2022/2556 (14. detsember 2022) ülevõtmiseks esitada Vabariigi Valitsusele hiljemalt 2024. aasta juuliks[3].

Eelnõuga muudetakse:
- finantskriisi ennetamise ja lahendamise seadust (edaspidi *FELS*) redaktsioonis RT I, 17.03.2023, 7;
- Finantsinspektsiooni seadust (edaspidi *FIS*) redaktsioonis RT I, 30.11.2022, 14;
- investeerimisfondide seadust (edaspidi *IFS*) redaktsioonis RT I, 17.03.2023, 9;
- hoiu-laenuühistute seadust (edaspidi *HLÜS*) redaktsioonis RT I, 05.05.2022, 12;
- kindlustustegevuse seadust (edaspidi *KindlTS*) redaktsioonis RT I, 17.03.2023, 11;
- krediidiasutuste seadust (edaspidi *KAS*) redaktsioonis RT I, 17.03.2023, 16;
- makseasutuste ja e-raha asutuste seadust (edaspidi *MERAS*) redaktsioonis RT I, 17.03.2023, 18
- väärtpaberite registri pidamise seadust (edaspidi *EvKS*) redaktsioonis RT I, 17.03.2023, 11;
- väärtpaberituru seadust (edaspidi *VpTS*) redaktsioonis RT I, 17.03.2023, 30.

Eelnõu on seotud järgmiste EL õigusaktidega:
- DORA määrus;
- DORA direktiiv.

DORA määrus on lisaks seotud järgmiste EL õigusaktidega (vt seletuskirja punkti 2.5):
- Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (edaspidi ***NIS2 direktiiv***) ja
- Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2557, mis käsitleb elutähtsa teenuse osutajate toimepidevust ja millega tunnistatakse kehtetuks nõukogu direktiiv 2008/114/EÜ (edaspidi ***CER direktiiv***).

CER direktiivi ülevõtmiseks on Riigikantselei välja töötanud hädaolukorra seaduse ja teiste seaduste muutmise seaduse eelnõu[4].

Eelnõu vastuvõtmiseks on vajalik Riigikogu poolthäälte enamus.

2. Seaduse eesmärk

2.1. Eelnõu algatamise vajalikkus

Seaduse eesmärk on tagada DORA määruse ja DORA direktiivi nõuetekohane riigisisene rakendamine. Kuivõrd finantsasutused sõltuvad oma igapäevases äritegevuses suurel määral digitehnoloogia kasutamisest, on oluline, et nad tagavad digitaalse tegevuskerksuse IKT-riski suhtes.

[3] VVTP-s on viide direktiivile (EL) 2022/1556, õige on (EL) 2022/2556.

[4] https://eelnoud.valitsus.ee/main/mount/docList/ad7af8cd-617c-45f3-b850-78ad002f6a3a

Kogu finantssektori IKT-riski ja tegevuskerksust hõlmav ELi õigusraamistik on killustunud ega ole täielikult järjepidev. Kuigi EL tasandil on IKT-riskiga seotud nõudeid (osana operatsiooniriski nõuetest) käsitletud näiteks Euroopa Parlamendi ja nõukogu direktiivides 2009/65/EÜ[5], 2009/138/EÜ[6], 2011/61/EL[7], 2013/36/EL[8], 2014/59/EL[9], 2014/65/EL[10], (EL) 2015/2366[11] ja (EL) 2016/2341[12], on need nõuded väga erinevad ja kohati mittetäielikud. Kuigi viidatud liidu õigusaktides on käsitletud operatsiooniriski norme põhjalikumalt, on keskendutud sageli traditsioonilisele kvantitatiivsele riski käsitlevale lähenemisviisile (kehtestades riski hõlmamiseks kapitalinõuded), mitte sihipärastele kvalitatiivsetele normidele, millega nähakse ette kaitsmise, avastamise, piiramise, taastamise ja parandamise suutlikkus IKT-ga seotud intsidentide puhul või teatamise ja digitaalse testimise suutlikkus. Lisaks, kuna IKT-ga seotud intsidentidest teatamise nõuded ei ole järjepidevad, ei ole ka järelevalveasutustel täielikku ülevaadet intsidentide laadist, sagedusest, tähtsusest ja mõjust.

Finantsinspektsiooni 2. novembri 2022. aasta pressiteates[13] on osutatud, et „väikepankade või nende teenusepakkujate vastu suunatud küberrünnete hulk kasvas 2021. aastal võrreldes aasta varasemaga ligi kolm korda. 2022. aasta alguses alanud Ukraina-Vene sõjaga seoses on rünnakute oht jätkuvalt kõrge nii pankade enda kui ka nende teenuste toimimist mõjutavate oluliste teenusepakkujate süsteemide vastu. FI-le edastatud info kohaselt hindavad väikepangad keskmisest kõrgemaks riski, mis on seotud IT tegevuste edasiandmisega. Mida rohkem kasutavad väikepangad IT-ga seotud tegevustel väliseid partnereid, seda suuremad on ka riskid. Kuna Eesti pangad pakuvad teenuseid peamiselt läbi e-kanalite, siis on ka e-kanalite talitluspidevusega seotud riskid keskmisest kõrgemad. Lisaks teatasid mitmed tarkvaratootjad eelmisel aastal olulistest turvanõrkustest laialdaselt kasutatavates tarkvarades, millele tuli pankadel kaasneva riski vältimiseks kiirelt reageerida ning vajalikke meetmeid rakendada“.

Euroopa Süsteemsete Riskide Nõukogu (ESRB) kinnitas süsteemset küberriski käsitlevas 2020. aasta aruandes[14], et finantssektori ettevõtjate, finantsturgude ja finantsturutaristu suur omavaheline seotus ning eelkõige nende IKT-süsteemide omavaheline sõltuvus võivad kujutada endast süsteemset nõrkust, sest lokaalsed küberintsidendid võivad kanduda kiiresti EL mis tahes ühest ligikaudu 22 000 finantssektori ettevõtjast üle kogu finantssüsteemile, olenemata geograafilistest piiridest. Finantssektoris toimuvad tõsised IKT-ga seotud

---

5 Euroopa Parlamendi ja nõukogu direktiiv 2009/65/EÜ, 13. juuli 2009 , vabalt võõrandatavatesse väärtpaberitesse ühiseks investeeringuks loodud ettevõtjaid (eurofondid) käsitlevate õigus- ja haldusnormide kooskõlastamise kohta EMPs kohaldatav tekst

6 Euroopa Parlamendi ja Nõukogu direktiiv 2009/138/EÜ, 25. november 2009 , kindlustus- ja edasikindlustustegevuse alustamise ja jätkamise kohta (Solventsus II) EMPs kohaldatav tekst

7 Euroopa Parlamendi ja nõukogu direktiiv 2011/61/EL, 8. juuni 2011 , alternatiivsete investeerimisfondide valitsejate kohta, millega muudetakse direktiive 2003/41/EÜ ja 2009/65/EÜ ning määruseid (EÜ) nr 1060/2009 ja (EL) nr 1095/2010 EMPs kohaldatav tekst

8 Euroopa Parlamendi ja nõukogu direktiiv 2013/36/EL, 26. juuni 2013 , mis käsitleb krediidiasutuste tegevuse alustamise tingimusi ning krediidiasutuste ja investeerimisühingute usaldatavusnõuete täitmise järelevalvet, millega muudetakse direktiivi 2002/87/EÜ ning millega tunnistatakse kehtetuks direktiivid 2006/48/EÜ ja 2006/49/EÜ EMPs kohaldatav tekst

9 Euroopa Parlamendi ja nõukogu direktiiv 2014/59/EL, 15. mai 2014 , millega luuakse krediidiasutuste ja investeerimisühingute finantsseisundi taastamise ja kriisilahenduse õigusraamistik ning muudetakse nõukogu direktiivi 82/891/EMÜ ning Euroopa Parlamendi ja nõukogu direktiive 2001/24/EÜ, 2002/47/EÜ, 2004/25/EÜ, 2005/56/EÜ, 2007/36/EÜ, 2011/35/EL, 2012/30/EL ja 2013/36/EL ning määruseid (EL) nr 1093/2010 ja (EL) nr 648/2012 EMPs kohaldatav tekst

10 Euroopa Parlamendi ja nõukogu direktiiv 2014/65/EL, 15. mai 2014 , finantsinstrumentide turgude kohta ning millega muudetakse direktiive 2002/92/EÜ ja 2011/61/EL (uuesti sõnastatud) EMPs kohaldatav tekst

11 Euroopa Parlamendi ja nõukogu direktiiv (EL) 2015/2366, 25. november 2015, makseteenuste kohta siseturul, direktiivide 2002/65/EÜ, 2009/110/EÜ ning 2013/36/EL ja määruse (EL) nr 1093/2010 muutmise ning direktiivi 2007/64/EÜ kehtetuks tunnistamise kohta (EMPs kohaldatav tekst)

12 Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/2341, 14. detsember 2016, tööandja kogumispensioni asutuste tegevuse ja järelevalve kohta (uuesti sõnastatud) (EMPs kohaldatav tekst)

13 https://fi.ee/et/uudised/finantsinspektsioon-suunab-panku-maandama-it-riske

14 https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

rikkumised ei mõjuta ainult üksikuid finantssektori ettevõtjaid. Need soodustavad ka lokaalselt nõrkuse edasi kandumist finantsülekannete kanaleid pidi ja võivad avaldada negatiivset mõju EL finantssüsteemi stabiilsusele, näiteks põhjustades likviidsuse väljavoolu ning üldiselt vähendada kindlustunnet ja usaldust finantsturgudesse.

Ka 2023. aasta ESRB raportis[15] on välja toodud, et geopoliitiline olukord on küberohu keskkonda oluliselt tõstnud.

2.2. Ülevaade finantsasutustele kohalduvatest digitaalse tegevuskerksuse nõuetest

A. IKT-riskide juhtimisraamistik

IKT-risk – mõistlikult tuvastatav asjaolu võrgu- ja infosüsteemide kasutamisel, mis realiseerumise korral võib seada ohtu:
- võrgu- ja infosüsteemi,
- tehnoloogiast sõltuva vahendi või protsessi,
- operatsiooni ja protsessi toimimise või
- teenuste osutamise turvalisuse,

tekitades kahjulikke mõjusid digitaalses või füüsilises keskkonnas.

IKT-riskide juhtimisraamistiku märksõnad	
Tuvasta	Finantsasutused määravad kindlaks, liigitavad ja dokumenteerivad asjakohaselt kõik IKT-põhised ärifunktsioonid, rollid ja vastutusvaldkonnad, neid funktsioone toetavad teabevara ja IKT-vara ning nende rollid ja sõltuvuse seoses IKT-riskidega.
Kaitse ja enneta	Finantsasutused seiravad ja kontrollivad pidevalt IKT-süsteemide ja -vahendite turvalisust ja toimimist ning minimeerivad IKT-süsteemidele avalduva IKT-riski mõju. Infoturbe korraga määratakse kindlaks reeglid andmete, teabevara ja IKT-vara kättesaadavuse, autentsuse, tervikluse ja konfidentsiaalsuse kaitsmiseks.
Avasta	Finantsasutusel peavad olema mehhanismid, mis võimaldavad kohe avastada anomaalset tegevust, sealhulgas IKT-võrgu jõudluse probleeme ja IKT intsidente, ning teha kindlaks võimalikud olulised nõrgad lülid.
Reageeri ja taasta	IKT talitluspidevuse põhimõtte eesmärk on tagada kriitilise tähtsusega või oluliste funktsioonide jätkumine, reageerida kõigile IKT intsidentidele ja lahendada need kiiresti; aktiveerida viivitamata piiramis-, reageerimis- ja taastemeetmed, hinnata mõju ning rakendada kommunikatsiooni- ja kriisijuhtimismeetmed. Finantsasutusel on kehtestatud IKT talitluspidevuse, reageerimis- ja taastekavad. Raamistiku osana töötatakse välja varunduspõhimõtted ja -menetlused, ennistamise ja taastamise menetlused ja meetodid, tagamaks IKT-süsteemide ja andmete ennistamine minimaalse seisuaja, piiratud katkestuse ja kaoga.
Õpi ja arene	Finantsasutusel peab olema suutlikkus ja personal, et koguda teavet nõrkuste, küberohtude ja IKT intsidentide, eelkõige küberrünnete kohta, ning analüüsida mõju, mida need võivad avaldada nende digitaalsele tegevuskerksusele. Personali koolituskavade raames töötatakse välja kohustuslike moodulitena IKT-turbe teadlikkuse suurendamise programmid

[15] https://www.esrb.europa.eu/pub/pdf/reports/esrb.macroprudentialtoolscyberresilience220214~984a5ab3a7.en.pdf?888a06fcb36d2c1ce41594efd67a4c88

	ja digitaalse tegevuskerksuse koolituse. Jälgida tuleb pidevalt ka tehnoloogia arengut, muu hulgas selleks, et mõista uue tehnoloogia võimalikku mõju IKT turvanõuetele ja digitaalsele tegevuskerksusele.
Suhtle	Finantsasutus koostab kriisikommunikatsioonikavad, mis võimaldavad teha klientidele ja vastaspooltele ning kohasel määral ka üldsusele vastutustundlikult teatavaks vähemalt tõsiseid IKT intsidente või nõrkusi. Personali kommunikatsioonipoliitikas võetakse arvesse vajadust eristada töötajaid, kes osalevad IKT-riski juhtimises (eelkõige reageerimise ja taaste eest vastutavaid töötajaid), ja töötajaid, keda tuleb teavitada.

B. IKT-ga seotud intsidendid ja küberohud ning nendest teavitamine

IKT-ga seotud intsident	Finantsasutuse poolt planeerimata üksiksündmus või omavahel seotud sündmuste jada, mis seab ohtu võrgu- ja infosüsteemide turvalisuse ning mis avaldab negatiivset mõju andmete konfidentsiaalsusele, kättesaadavusele, terviklusele ja autentsusele või finantssektori ettevõtja osutatavatele teenustele.
Tõsine IKT-ga seotud intsident	IKT-ga seotud intsident, millel on suur negatiivne mõju võrgu- ja infosüsteemidele, mis toetavad finantssektori ettevõtja kriitilise tähtsusega või olulisi funktsioone.
Küberoht	Võimalik asjaolu, sündmus või tegevus, mis võib kahjustada või häirida võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid või neile muul viisil halba mõju avaldada.
Oluline kübeoht	Küberoht, mille tehnilised tunnused näitavad, et selle tulemuseks võib olla IKT-ga seotud oluline intsident või tegevust või turvalisust mõjutav maksetega seotud oluline intsident.
Finantsasutuse kohustus:	- teavitada koheselt kliente, kui intsident neid mõjutab (finantshuvi); - teavitada viivitamata FI-d, mille alusel FI hindab intsidendi tähtsust ja piiriülest mõju (liikmesriigi valik – CSIRTi teavitamine); - edastada FI-le vaheraport ja lõppraport, sealjuures vaheraport tuleks esitada niipea, kui algse intsidendi staatus on oluliselt muutunud või intsidendi käsitlemine on uue kättesaadava teabe põhjal muutunud. Lõppraport esitatakse, kui analüüs on lõpule viidud, kuid see ei eelda, et kõiki maandamismeetmeid on juba ka rakendatud. - saab otsustada olulise küberohu korral ise, kas teavitab kliente ja pädevaid asutusi.
FI kohustus:	- teavitada finantsasutust, et ta on teate kätte saanud. - teavitada intsidendist Euroopa Järelevalveasutusi (ESA-sid), Euroopa Keskpanka (EKP) (asjakohasel juhul), riiklikke pädevaid asutusi, CSIRTe, kriisilahendusasutusi ja muid asutusi vastavalt riigisisesele õigusele.
FI võib:	- esitada tagasiside või anda kõrgetasemelisi suuniseid finantsasutusele, tehes eelkõige kättesaadavaks asjakohast anonüümitud teavet ja teadmust sarnaste ohtude kohta, ning võib arutada parandusmeetmeid, mida kohaldatakse finantsasutuse tasandil, ja viise negatiivse mõju minimeerimiseks ja leevendamiseks kogu finantssektorile.

C. Digitaalse tegevuskerksuse testimine

Milleks testitakse?	IKT-riskide juhtimisraamistiku osana tuleb luua digitaalse tegevuskerksuse testimise kava, selleks et: - hinnata valmisolekut intsidentide käsitlemiseks; - tuvastada nõrgad kohad ja puudused süsteemides ja inimressursis; - rakendada vajadusel parendusmeetmeid.
Kuidas testitakse?	Finantsasutus peab läbi viima järgmised testimised: - nõrkuse hindamised ja skaneerimised; - avatud lähtekoodiga tarkvara analüüsid; - võrguturvalisuse hindamised; - lünkade analüüsid; - füüsilise turvalisuse läbivaatamised; - küsimustikud ja skaneerimistarkvara lahendused; - võimaluse korral lähtekoodi ülevaatus; - stsenaariumipõhised testid; - ühilduvuse testimine ja jõudlustestid; - läbiv- ja läbistustestimine; - jne.
Mida/keda testitakse?	Testitakse nii süsteeme, IKT-vahendeid jne, aga ka töötajaid.
Mis on süvatestimine?	IKT süsteemide, protsesside ja vahendite süvatestimine: - ohuteabel põhinev läbistustestimine (küberrünnete matkimine); - iga 3a tagant (pädev asutus võib sagedust muuta); - pädev asutus määrab testimises osalevad finantsasutused (välistatud mikroettevõtjad ja need, kes kuuluvad leebema IKT riskijuhtimise režiimi alla); - testimine toimub *live* keskkonnas; - lubatud nii välised testijad kui ka teatud tingimustel sisetestijad; - testis osalevad ka kolmandast isikust IKT teenuseosutajad; - *Single public authority* (LR võib määrata ühe asutuse, kes vastutab testimisega seotud teemade eest); - testimise tulemustest teavitatakse seda asutust, kes omakorda väljastab tõendi, et testimine oli nõuetekohane.

D. Kolmanda isikuga seotud IKT-riskide juhtimine (IKT-teenuseosutajad)

Põhilised nõuded seoses kolmanda isikuga seotud IKT-riskide juhtimisega:

- nõuded IKT-teenuse edasiandmisele/lepingutele (uutele);
- teaberegister lepingute kohta, sealjuures eristades kriitilise tähtsusega või olulisi funktsioone toetavaid IKT-teenuseid käsitlevaid lepinguid muudest lepingutest;
- FI teavitamine – kord aastas uutest lepingutest ning kohene teavitus lepingu kavatsusest, kui IKT-teenus toetab kriitilise tähtsusega või olulisi funktsiooni;
- infoturbestandarditele vastavus. Finantsasutus võib sõlmida lepingu IKT teenuseosutajaga, kes vastab asjakohastele infoturbestandarditele. Rangemad nõuded teenuseosutajale, kui teenus toetab kriitilise tähtsusega ja olulisi funktsioone.
- väljumisstrateegia (alternatiivid teenuseosutaja kiireks asendamiseks);
- peamised lepingutingimused – teenuste kirjeldus, teenuse osutamise ja andmete talletamise asukoht, isikuandmete kaitse, tähtajad ja kohustused, kohustus pakkuda selle teenuseosutajaga seotud intsidendi korral tasuta või eelnevalt kokkulepitud hinnaga abi,

õigus jälgida teenusosutaja tegevust, kohustus teha koostööd pädeva asutusega, lepingu lõpetamise õigused, väljumisstrateegiad, osalemine testimisel jne;
- eraldi ametikoht;
- kui lepingud on tehniliselt väga keerukad, kontrollib finantsasutus, kas audiitoritel on piisavad oskused ja teadmised asjaomaste auditite ja hindamiste tõhusaks läbiviimiseks.

E. Järelevaatamine kriitilise tähtsusega kolmandast isikust IKT teenuseosutaja üle

Kuivõrd tegevuse edasiandmise ja kolmandast isikust IKT teenuseosutajate kontsentratsiooniga võib kaasneda potentsiaalne süsteemne risk ning kuna riiklikud mehhanismid ei ole piisavad, et tagada finantsjärelevalveasutustele asjakohased vahendid kriitilise tähtsusega kolmandast isikust IKT teenuseosutajate IKT-riskide tagajärgede kvantifitseerimiseks, kvalifitseerimiseks ja leevendamiseks, on DORA määrusega kehtestatud järelevaatamisraamistik, mis võimaldab finantsjärelevalveasutustel pidevalt seirata selliste teenuseosutajate tegevust.

Järelvaatamisfoorum (*Oversight Forum*)	Määrab, milline IKT teenuseosutaja on kriitilise tähtsusega.
	Määrab igale kriitilise tähtsusega teenuseosutajale juhtiva järelevaatamisasutuse, kelleks on üks ESA-dest.
Juhtiv järelevaatamisasutus (*Lead Overseer*)	Hindab, kuidas IKT teenuseosutaja juhib nõuetekohaselt IKT riske, millel võib olla mõju finantsasutusele.
	IKT teenuseosutajate peamine kontaktpunkt.
	Võtab vastu koostöös järelevaatamisvõrgustikuga järelevaatamise plaani iga kriitilise teenuseosutaja kohta.
	Küsib IKT teenuseosutajalt teavet, aruandeid, annab soovitusi.
	Viib läbi uurimisi ja kontrolle (moodustatakse *joint examination team*).
	Saab määrata IKT teenuseosutajale karistusi.
Järelevaatamisvõrgustik (*Joint Oversight Network*)	Võrgustikku kuuluvad kolm juhtivat järelevaatamisasutust ehk kõik ESA-d.
	Järelevaatamise koordineerimine ja rakendatavate õiguste ühtlustamine.

F. DORA rakendamiseks vajalikud regulatiivsed ja rakenduslikud standardid

Kuna DORA määrust hakkavad täiendama ESA-de poolt välja töötatud regulatiivsed ja rakenduslikud tehnilised standardid, on järgnevalt esitatud, mis kuupäevadeks peavad ESA-d vastavate standardite eelnõud Euroopa Komisjonile esitama. Standardite eelnõud peaksid aitama finantsasutustel DORA rakendamiseks vajalikke ettevalmistusi paremini planeerida juba enne DORA rakendumistähtaega.

17. jaanuar 2024. a.	- IKT juhtimisraamistiku nõuete täpsustamine (art 15). - Lihtsustatud IKT juhtimisraamistiku nõuete täpsustamine (art 16). - IKT intsidentide liigitamise kriteeriumid, oluliste küberohtude kindlaksmääramise kriteeriumid ja tõsiste IKT intsidentide olulisuse hindamise kriteeriumid teistele pädevatele asutustele (art 18). - Teaberegistri standardvorm, üksikasjad seoses kolmanda isikuga seotud lepingutega, mis käsitlevad kriitilisi ja olulisi funktsioone toetavaid IKT teenuseid (art 28).

17. juuli 2024. a.	- IKT intsidentide teavitamise vormid ja menetlused, raportite sisu ja esitamise tähtajad, küberohtusid käsitletava teabe sisu (art 20). - Süvatestimise kohaldamisala kriteeriumid, nõuded sisetestijatele, testimismetoodika ja meetodid, testimise etapid, koostöö vastastikuse tunnustamise jaoks (art 26). - IKT teenuseosutaja alltöövõtulepinguga seotud tingimused (art 30). - Järelevaatamise tingimused, sh kriitilisele IKT teenuseosutajale (art 41).

2.3. Väljatöötamiskavatsus ja valikukohad
2.3.1. Väljatöötamiskavatsus

Väljatöötamiskavatsust ei ole koostatud tulenevalt hea õigusloome ja normitehnika eeskirja § 1 lõike 2 punktist 2, kuivõrd eelnõu käsitleb EL õiguse rakendamist.

DORA määruse ja direktiivi eelnõuga koos koostas Euroopa Komisjon mõjuanalüüsi[16]: „Impact assessment report – Accompanying the Document – Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014."

2.3.2. Valikukohad

A. DORA määruse valikukoht 1. Tõsistest IKT-ga seotud intsidentidest teavitamine ja olulistest küberohtudest teavitamine.

Art 19 lg 1. „Finantssektori ettevõtjad teavitavad tõsistest IKT intsidentidest artiklis 46 osutatud asjaomasele pädevale asutusele kooskõlas käesoleva artikli lõikega 4. /…./ Ilma et see piiraks finantssektori ettevõtja poolset esimese lõigu kohast asjaomase pädeva asutuse teavitamist, võivad liikmesriigid lisaks otsustada, et mõned või kõik finantssektori ettevõtjad esitavad pädevale asutusele või küberturbe intsidentide lahendamise üksustele, mis on määratud või loodud direktiivi (EL) 2022/2555 kohaselt[17], ka esialgse teate ja kõik raportid, millele on osutatud käesoleva artikli lõikes 4, kasutades artiklis 20 osutatud vorme."

Art 19. lg 2. „Finantssektori ettevõtjad võivad vabatahtlikult teatada asjaomasele pädevale asutusele olulistest küberohtudest, kui nad peavad ohtu finantssüsteemi, teenusekasutajate või klientide jaoks oluliseks. /…/ Liikmesriigid võivad otsustada, et need finantssektori ettevõtjad, kes teatavad vabatahtlikult esimese lõigu kohaselt, võivad kõnealuse teate edastada ka direktiivi (EL) 2022/2555 kohaselt määratud või loodud küberturbe intsidentide lahendamise üksustele."

DORA määruse põhjenduspunktis 52 on selgitatud, et „lisaks peaks liikmesriikidel olema võimalik kindlaks määrata, et finantssektori ettevõtjad peaksid ise esitama sellist teavet avaliku sektori asutustele, mis ei kuulu finantsteenuste valdkonda. Need teabevood peaksid võimaldama finantssektori ettevõtjatel kiiresti saada kasu kõnealuste asutuste asjakohasest tehnilisest panusest, nõuannetest parandusmeetmete kohta ja edasistest järelmeetmetest."

Vabariigi Valitsuse 17. detsembri 2020. aasta istungil kiideti heaks Eesti seisukohad EL digirahanduse paketi kohta[18], sealhulgas finantsteenuste digitaalse tegevuskerksuse

[16] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0198

[17] NIS2 direktiiv

[18] https://eelnoud.valitsus.ee/main/mount/docList/c969654c-9691-4b71-abb1-7baa3e665d13

regulatsiooni kohta. Muu hulgas kiideti heaks seisukoht, et DORA määruse ettepanekus kavandatud teavitamisnõuded peavad olema piisavalt paindlikud, et nõudeid saaks riigid erinevate institutsionaalsete struktuuride korral ja teavitamiskohustusega subjektide suhtes halduskoormust suurendamata säästlikult rakendada, sealhulgas järgides ühekordse teabe edastamise või küsimise põhimõtet, et operatiivne info küberintsidendi kohta vajalikus ulatuses ja mahus jõuaks viivitusteta asjaomaste riiklike pädevate asutusteni, sealhulgas küberturbe intsidentide lahendamise üksuseni.

Tulenevalt DORA määruses ette nähtud liikmesriigi võimalusest, valitsuse positsioonist ja huvirühmadega konsulteerimisel esitatud seisukohtades, on eelnõus võetud lähenemine, et finantsasutus teavitab tõsistest intsidentidest ühekordse edastamisviisiga nii FI-d kui ka RIA-t, kasutades selleks sama teavitusvormi (sama teavitusnormi kasutamine tuleb määrusest). Lisaks, kui finantsasutus on otsustanud teavitada FI-d olulisest küberohust, teavitab ta sellest ka RIA-t.

B. DORA määruse valikukoht 2. Ohutabel põhineva läbistustestimise eest vastutav riiklik asutus.

Art 26 lg 9. „Liikmesriigid võivad määrata finantssektoris ühe avaliku sektori asutuse, kes vastutab riiklikul tasandil ohuteabel põhineva läbistustestimisega seotud küsimuste eest finantssektoris, ning annavad talle kõik selleks vajalikud volitused ja ülesanded.“

Põhjenduspunkt 58 selgitab lisaks, et selleks, et tugineda teatavate pädevate asutuste poolt juba omandatud eksperditeadmistele, eelkõige seoses TIBER-EU raamistiku rakendamisega, peaks määrus võimaldama liikmesriikidel määrata ühe avaliku sektori asutuse, kes vastutab riiklikul tasandil kõigi ohuteabel põhinevate läbistustestidega seotud küsimuste eest finantssektoris, või pädevad asutused, kes sellise määramise puudumisel delegeeriksid ohuteabel põhinevate läbistustestidega seotud ülesannete täitmise mõnele muule riiklikule finantssektori pädevale asutusele.

Kuna üldine printsiip on, et FI on järelevalve eest vastutav asutus finantssektoris (mh IT/küber küsimused, mis on tavapärane järelevalveline osa), siis on ka eelnõu koostamisel võetud lähenemine, et artikli 26 lõike 9 kohaselt ei määrata eraldi asutust, kes vastutab ohuteabel põhinevate läbistustestidega seotud küsimuste eest finantssektoris, kuid koostöösätetega tagatakse, et FI teeb RIA-ga koostööd, muu hulgas seoses finantsasutuste ohuteabel põhinevate läbistustestimistega. Võttes arvesse RIA küberkerksuse kompetentsi ning asjaolu, et tegemist on KüTS kohaselt ka küberturvalisuse pädeva asutusega, on oluline tagada hea ja sujuv koostöö, et finantsasutuste testimised viiakse läbi nõuetekohaselt ja tänu teabe vahetamisele on asutustel olemas kogu vajalik teave nii testide läbiviimise kui ka tulemuste kohta.

Siinjuures on oluline juhtida tähelepanu asjaolule, et kuna oluliste krediidiasutuste puhul on pädevaks asutuseks Euroopa Keskpank, kelle järelevalve alla kuulub 1. märtsi 2023. a seisuga 110 institutsiooni, neist 4 Eesti krediidiasutust ning süvatestimise kohustus on eelkõige olulistel krediidiasutustel[19], siis artikli 26 lõike 9 kohaselt muu vastutava asutuse määramine teatud ülesannete täitmiseks võib pigem järelevalve rolli, õigusi ja terviklikkust hägustada.

C. DORA määruse valikukoht 3. Hoiu-laenuühistutele DORA kohaldamine.

[19] See veel selgub, millised finantsasutused peavad süvatestimisi läbi viima, kuid eelduslikult on nendeks näiteks olulised pangad ja börs.

Art 2 lg 4. „Liikmesriigid võivad käesoleva määruse kohaldamisalast välja arvata direktiivi 2013/36/EL artikli 2 lõike 5 punktides 4–23 osutatud üksused, mis asuvad nende vastaval territooriumil. Kui liikmesriik otsustab vastavale asutusele DORA määrust kohaldada, siis kohaldub neile IKT-riskide juhtimisraamistiku lihtsustatud režiim."

Direktiivi 2013/36/EL artikli 2 lõike 5 punktis 6 on viidatud Eesti puhul hoiu-laenuühistutele, mis on hoiu-laenuühistu seaduse kohaselt tunnustatavad ühistud.

Seega kohalduvad DORA määruses sätestatud digitaalse tegevuskerksuse nõuded mh hoiu-laenuühistutele ning vaid juhul, kui liikmesriik otsustab rakendada DORA määruse artikli 2 lõike 4 valikut, jäävad hoiu-laenuühistud DORA määruse alt välja. Konsulteerides huvirühmadega, selgus, et DORA nõuete kohaldamine hoiu-laenuühistutele oleks asjakohane, kuid see eeldaks, et nad on finantsjärelevalve subjektid. Kuna hoiu-laenuühistud ei ole finantsjärelevalve subjektid, on nende suhtes keeruline DORA määruse nõudeid kohaldada, kuna suur osa sätteid on seotud pädeva asutuse rolliga (intsidentidest teavitamine jne), mistõttu on käesoleva eelnõu puhul võetud lähenemine, et käesoleval hetkel nende suhtes DORA määruse nõuded ei kohaldu.

Samas, kui liikmesriik otsustab hoiu-laenuühistu jätta DORA määruse kohaldamisalasse, siis DORA määruses sätestatud nõuete täitmise üle peaks määruse artikli 46 kohaselt järelevalvet teostama sama asutus, kes on ka krediidiasutuse pädev asutus ehk selleks peaks olema FI.

Eelnõu väljatöötamisel oli kaalumisel ka variant, et kui hoiu-laenuühistud jätta DORA määruse kohaldamisalast välja, siis alternatiivina oleks võimalik neile ka KüTS küberturvalisuse nõudeid kohaldada ja RIA oleks sellisel juhul pädevaks asutuseks. Kuna hoiu-laenuühistute seaduseelnõu[20] menetlus on hetkel veel pooleli, siis hetkel on võetud lähenemine, et sõltuvalt menetluse seisust ja tulemusest seoses viidatud eelnõuga, tehakse otsused ka selles osas, mis puudutab hoiu-laenuühistutele küberturvalisuse nõuete kohaldamist.

D. DORA määruse valikukoht 4. Kriminaalkaristused

Art 52 lg 1. Liikmesriigid võivad otsustada mitte kehtestada halduskaristusi või parandusmeetmeid käsitlevaid õigusnorme selliste rikkumiste suhtes, mille suhtes kohaldatakse nende riiklikus õiguses kriminaalkaristusi.

Kuna analoogne liikmesriigi otsustuskoht on ka teistest EL finantssektori direktiivides ja määrustes ning Eesti puhul on võetud lähenemine mitte seda valikut rakendada, siis on otsustad ka käesoleva eelnõu raames jääda sellise lähenemise juurde.

E. DORA pädev asutus

Tegemist ei ole otseselt liikmesriigi valikukohaga, kuid huvirühmadega konsultatsiooni käigus tõstatus teema, milline asutus peaks olema pädev asutus DORA määruses sätestatud ülesannete täitmisel ja järelevalve teostamisel. Tehti ettepanek kaaluda varianti, et RIA on pädev asutus kübervaldkonda puudutavas osas ja FI muudes teemades, mis ei eelda küberkompetentsi.

DORA pädev asutus on määratletud DORA määruse artiklis 46. Tegemist on sama asutusega, kes teostab finantsasustuse üle finantsjärelevalvet. Nimelt on DORA määruse artiklis 46 viited finantssektori EL direktiividele ja määrustele, mis reguleerivad finantsasutuste tegevust ja järelevalvet. Liikmesriik on pidanud määrama pädeva asutuse, kes teostab EL finantssektori

[20] https://eelnoud.valitsus.ee/main/mount/docList/db5ae432-6d08-4896-972c-101c32e9d2ce

direktiivides ja määrustes sätestatud nõuete täitmise üle järelevalvet. Eestis teostab artiklis 46 viidatud EL direktiivides ja määrustest sätestatud nõuete täitmise üle järelevalvet FI. Oluliste krediidiasutuste puhul on pädevaks asutuseks Euroopa Keskpank. Selleks, et anda DORA pädeva asutuse roll osaliselt RIA-le, tuleb RIA määratleda (kaas)pädeva asutusena ka kõikide artiklis 46 loetletud finantssektori EL direktiivide ja määruste tähenduses. Selline lähenemine omakorda tähendab, et viidatud EL direktiivide ja määruste kohaselt määratav pädev asutus on ka osa Euroopa Finantsjärelevalve Süsteemist. Pädeval asutusel on rida kohustusi Euroopa Järelevalveasutuste ees, sh osamaksete tasumise kohustus.

Asjaolu, et DORA määruse pädevaks asutuseks otsustati DORA määruse väljatöötamisel määrata sama asutus, kes vastutab finantsjärelevalve eest, tuleneb eelkõige sellest, et sellise lähenemise eesmärk on tagada, et finantsjärelevalve asutusel oleks tervikpilt kõikidest riskidest, millega finantsasutus kokku puutub, sh IKT-riskidest. IKT riskide juhtimine on osa finantsasutuse riskijuhtimissüsteemist. Riskipõhiste kapitalinõuete puhul ka osa kapitalijuhtimisest. Samuti on IKT-teenuste edasiandmine osa finantsasutuse teenuste ja tegevuste edasiandmise raamistikust. Finantssektor on terviklik, mida tuleb vaadelda kompaktselt ning pädevuse jagamine teatud teemade osas ei ole võimalik, et tagada järjepidev, stabiilne ja usaldusväärne finantssektor. FIS § 3 kohaselt teostab Finantsinspektsioon riiklikku finantsjärelevalvet finantssektori stabiilsuse, usaldusväärsuse ja läbipaistvuse ning toimimise efektiivsuse suurendamise, süsteemsete riskide vähendamise ning finantssektori kuritegelikel eesmärkidel ärakasutamise tõkestamisele kaasaaitamise eesmärgil, et kaitsta klientide ja investorite huve nende vahendite säilimisel ning seeläbi toetada Eesti rahasüsteemi stabiilsust. Selleks, et FI seda teha saaks, ongi vaja järelevalves terviklikku lähenemist.

DORA määrus näeb ette mitmeid võimalusi koostööks NIS2 pädeva asutusega. Eelnõus on ette nähtud uus FIS paragrahvi, mis reguleerib koostööd küberturvalisuse valdkonnas (vt selgitusi FIS § 47^{11} juures), mis annab võimaluse kaasata DORA nõuete järelevaatamisse ka RIA.

Teavitused tõsistest IKT-intsidentidest edastatakse mh RIA-le (vt valikukoht 1) ning DORA ei piira RIA võimalusi abistada finantsasutusi. Nimelt on DORA määruse artikli 22 lõike 1 sissejuhatavas osas selge viide sellele, et NIS2 pädeva asutus saab vastavalt liikmesriigi õigusele pakkuda finantsasutusele tehnilist panust, nõuandeid või parandusmeetmeid ning järelmeetmeid.

2.4. Sihtrühm

Sihtrühma kuuluvad Eestis tegevusloa või registreeringu alusel tegutsevad finantsasutused.

Tabelis 1 on välja toodud DORA määruse kohaldamisalasse kuuluvad ja mitte kuuluvad finantsasutused, Eestis asutatud finantsasutuste arv ja proportsionaalsuse rakendamise põhimõtted.

Finantsasutused	Arv	Proportsionaalsuse põhimõte:
Krediidiasutused	9	- mikrodele[21] leevendused ptk-des 2, 4 ja 5.
Makseasutused (sulgudes erandi alla kuuluvad asutused)	12 (4)	- mikrodele leevendused ptk-des 2, 4 ja 5. - leebem IKT-riskijuhtimise režiim (ptk 2) erandi alla kuuluvatele makseasutustele.
E-raha asutused	2	- mikrodele leevendused ptk-des 2, 4 ja 5.

[21] kus töötab vähem kui 10 inimest ning kelle aastakäive ja/või aastabilansi kogumaht ei ületa 2 miljonit eurot

		- leebem IKT-riskijuhtimise režiim (ptk 2) erandi alla kuuluvatele e-raha asutustele.
Kindlustusandjad	9	- mikrodele leevendused ptk-des 2, 4 ja 5.
Kindlustusmaaklerid, kellel hakkab DORA kohalduma (sulgudes maaklereid kokku)	0 (40)	- DORA määrus ei kohaldu mikrodele, väikestele[22] ja keskmise suurusega[23] kindlustusvahendajatele.
Kindlustusagendid, kellele hakkab DORA kohalduma (sulgudes agente kokku)	0 (362)	- DORA määruse ei kohaldu mikrodele, väikestele ja keskmise suurusega kindlustusvahendajatele.
Fondivalitsejad	11	- mikrodele leevendused ptk-des 2, 4 ja 5. - kohustusliku ja täiendava pensionifondi valitsejatele DORA ei kohaldu.
Tegevusloaga väikefondi valitsejad	(6)	- DORA määrus neile ei kohaldu.
Registreeritavad väikefondi valitsejad	(74)	- DORA määrus neile ei kohaldu.
Investeerimisühingud	9	- mikrodele leevendused ptk-des 2, 4 ja 5. - leebem IKT-riskijuhtimise režiim (ptk 2) väikestele ja mitteseotud investeerimisühingutele.
Reguleeritud turu korraldaja	1	- mikrodele leevendused ei kohaldu.
Väärtpaberiarveldussüsteemi korraldaja	1	- mikrodele leevendused ei kohaldu.
Väärtpaberituru kauplemiskohad	1	- mikrodele leevendused ei kohaldu.
Keskne vastaspool	0	- mikrodele leevendused ei kohaldu.
Aruandlusteenuse osutaja	0	- mikrodele leevendused ptk-des 2, 4 ja 5.
Ühisrahastusteenuse osutajad	2	- mikrodele leevendused ptk-des 2, 4 ja 5.
Hoiu-laenuühistud	21[24]	- leebem IKT-riskijuhtimise režiim (ptk 2). Eesti ei kohalda hoiu-laenuühistutele määrust.
Tööandja kogumispensioni asutused	0	- DORA määrus ei kohaldu IORP-dele, kus vähem kui 15 liiget. - leebem IKT-riskijuhtimise režiim (ptk 2) kuni 100 liikmega IORP-idele.
Krüptovarateenuse osutajad (MICAR tegevusloaga)	0[25]	- mikrodele leevendused ptk-des 2, 4 ja 5.
Varapõhiste tokenite emitendid (MICAR tegevusloaga)	0	- mikrodele leevendused ptk-des 2, 4 ja 5.

[22] töötab 10 või rohkem inimest, kuid vähem kui 50 inimest ja kelle aastakäive ja/või aastabilansi kogumaht ületab 2 miljonit eurot, kuid ei ületa 10 miljonit eurot

[23] kes ei ole väikeettevõtja ja kus töötab vähem kui 250 inimest ning kelle aastakäive ei ületa 50 miljonit eurot ja/või aastabilanss ei ületa 43 miljonit eurot

[24] https://statistika.eestipank.ee/failid/mbo/hly.html

[25] Käesoleval hetkel ei ole veel võimalik MICAR alusel tegevusluba taotleda. 2023. aasta mai seisuga on RahaPST alusel tegutsemas 94 virtuaalvääringuteenuse pakkujat.

Tabel 1. DORA kohaldamisalasse kuuluvate finantsasutuse arv.

DORA määruse kohaldamisalasse kuuluvad ka kriitilise tähtsusega kolmandast isikust IKT teenuseosutajad, kuid hetketeadmise kohaselt ükski Eesti ettevõtja pole määratletav kriitilisena. Näiteks on tegemist pilv-, tarkvara- ja andmeanalüüsiteenuste osutajate ning andmekeskuse teenuste osutajatega, kuid lisaks peavad olema täidetud mitmed kriitilise IKT teenuseosutaja kriteeriumid.

2.5. DORA määruse seos liidu tasandil kehtestatud horisontaalne küberturvalisuse raamistiku ja elutähtsa teenuseosutaja toimepidevuse nõuetega

EL Teatajas avaldati paralleelselt DORA määruse ja DORA direktiiviga NIS2 ning CER direktiivid. Samas, kui DORA nõudeid tuleb kohaldama hakata 17. jaanuarist 2025. a, siis NIS2 ja CER direktiivides on ette nähtud, et nendest direktiividest tulenevad nõuded kohalduvad 18. oktoobrist 2024.a.

Õiguse kohaldamine

Kuna NIS2 direktiivi ja CER direktiiviga on mh hõlmatud krediidiasutused, kauplemiskohad ja kesksed vastaspooled, on oluline üheselt aru saada, milliseid nõudeid ja mis ulatuses krediidiasutused, kauplemiskohad ja kesksed vastaspooled järgima peavad.

NIS2 direktiivi kohaldatakse direktiivi I või II lisas osutatud sellist liiki avalik-õiguslike või eraõiguslike üksuste suhtes, mis kvalifitseeruvad soovituse 2003/361/EÜ[26] lisa artikli 2 kohaselt keskmise suurusega ettevõtjateks või ületavad kõnealuse artikli lõikes 1 sätestatud keskmise suurusega ettevõtja piirmäärasid, ning osutavad teenuseid või tegutsevad liidus. NIS2 direktiivi I lisa punktides 3 ja 4 on kriitilise tähtsusega sektorina välja toodud pangandussektor ja finantsturutaristud. Samas kohaldatakse NIS2 direktiivi lisaks ka üksuste suhtes (olenemata nende suurusest), kui neid käsitatakse CER direktiivi kohaselt elutähtsa teenuse osutajatena (edaspidi ***ETO***) või kui üksuse osutatava teenuse häire võib tuua kaasa olulise süsteemse riski, eelkõige sektorites, kus sellisel häirel võib olla piiriülene mõju.

DORA määruse põhjenduspunktis nr 16 on selgitatud, et DORA määrus on NIS2 suhtes *lex specialis*. NIS2 direktiivi põhjenduspunkt 28 selgitab lisaks, et NIS2 direktiivi sätete asemel tuleks kohaldada DORA määruse sätteid, mis käsitlevad IKT riskijuhtimist, IKT intsidentide haldamist ja eelkõige tõsistest IKT intsidentidest teavitamist, samuti digitaalse tegevuskerksuse testimist, teabevahetuse kokkuleppeid ja kolmandatest isikutest tulenevat IKT-riski. Seetõttu ei tohiks liikmesriigid NIS2 direktiivi sätteid, mis käsitlevad küberturvalisuse riskijuhtimist ja teatamiskohustust, järelevalvet ja täitmise tagamist, DORA määruse kohaldamisalasse jäävate finantssektori ettevõtjate suhtes kohaldada.

CER direktiivi artikli 6 kohaselt identifitseerib liikmesriik elutähtsa teenuse osutajad sellistes valdkondades nagu pangandus, kauplemiskohad ja kesksed vastaspooled.

CER direktiivi põhjenduspunkt 21 selgitab, et kuna finantssektori ettevõtjate toimepidevus on põhjalikult hõlmatud DORA regulatsiooniga, ei tuleks selliste ettevõtjate suhtes kohaldada CER direktiivi artiklit 11 ning III, IV ja VI peatükki, et vältida dubleerimist ja ebavajalikku halduskoormust (vt ka artiklit 8). Lisaks selgitab viidatud põhjenduspunkt, et võttes arvesse finantssektori ettevõtjate poolt kõikidesse muudesse sektoritesse kuuluvate elutähtsate teenuse

[26] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32003H0361

osutajatele osutatavate teenuste olulisust, peaksid liikmesriigid CER direktiiviga ette nähtud kriteeriumide põhjal ja selles sätestatud menetlust kohaldades identifitseerima sellised finantssektori ettevõtjad elutähtsa teenuse osutajana ning kohaldama nende suhtes CER direktiivi II peatükis sätestatud strateegiaid, liikmesriigi riskianalüüse ja toetusmeetmeid.

Koostöö ja küberturvalisuse strateegia

DORA määrus võimaldab Euroopa järelevalveasutustel ja finantsjärelevalve pädevatel asutustel osaleda koostöörühma tegevuses ning vahetada teavet ja teha koostööd ühtsete kontaktpunktide[27], samuti küberturbe intsidentide lahendamise üksuste (CSIRT) ja küberturvalisuse pädevate asutustega. Näiteks peavad finantsjärelevalve pädevad asutused edastama tõsiste IKT intsidentide ja asjakohasel juhul oluliste küberohtude üksikasjad ka CSIRTidele, pädevatele asutusele või ühtsetele kontaktpunktidele. See saavutatakse vahetu juurdepääsu tagamisega intsidenditeadetele ja nende otsese või intsidenditeadete ühtse kontaktpunkti edastamise kaudu.

Lisaks peaksid liikmesriigid jätkuvalt kaasama finantssektori oma küberturvalisuse strateegiatesse ning CSIRTid võivad oma tegevuses hõlmata ka finantssektorit.

Kokkuvõte

	DORA	**CER** (ETO)	**NIS2 (**ETO ja keskmise suurusega või suurem ettevõtja)
Krediidiasutused ja finantsturutaristud	Kohaldub täies ulatuses.	Kohaldub CER direktiivi II peatükk; Ei kohaldata CER direktiivi art 11 ning III, IV ja VI peatükki.	Ei kohaldata IKT riskijuhtimist, IKT intsidentide haldamist ja nendest teavitamist, digitaalse tegevuskerksuse testimist, teabevahetuse kokkuleppeid ja kolmandatest isikutest tulenevate IKT-riskidega seotud sätteid.
Pädev asutus seoses krediidiasutuse ja finantsturutaristu järelevalvega	FI; EKP (olulised krediidiasutused).	FI/EKP, kui liikmesriik ei otsusta CER II peatüki pädeva asutuse kohustusi anda teisele pädevale asutusele.	RIA
Koostöö	FI/EKP õigus osaleda NIS2 art 14 koostöörühmas.	Koostöö NIS2 päeva asustusega.	Art 13 – RIA koostöö, sh teabe vahetamine DORA

[27] Iga liikmesriik määrab küberturvalisuse pädevate asutuste seast ühe kontaktpunkti, mis täidab sidepidamisfunktsiooni, et tagada oma liikmesriigi ametiasutuste piiriülene koostöö teiste liikmesriikide asjaomaste asutustega ning asjakohasel juhul komisjoni ja ENISAga ning ka valdkondadevaheline koostöö oma liikmesriigi teiste pädevate asutustega.

	FI teavitab tõsistest intsidentidest RIA-t ja asjakohasel juhul muid avaliku sektori asutusi. FI/EKP saab vajadusel konsulteerida RIA ja muu liikmesriigi NIS2 pädeva asutusega.	Kuna DORA pädev on teatud juhtudel ka CER pädev asutus, siis peab tegema koostööd ka teis(t)e CER pädeva (te) asutus(te)ga.	(FI/EKP) ja CER pädevate asutustega ja muude artiklis loetletud asutustega.

3. Eelnõu sisu ja võrdlev analüüs

3.1. Eelnõu § 1. Finantskriisi ennetamise ja lahendamise seaduse muutmine

Digitaalne tegevuskerksus on oluline, et säilitada finantsasutuse kriitilised funktsioonid ja põhiäriliinid kriisilahenduse korral ning seeläbi vältida häireid reaalmajanduses ja finantssüsteemis. Direktiivi 2014/59/EL muutmise eesmärgiks on tagada, et tegevuserksusega seotud teavet võetakse kriisilahenduse kavandamisel ning kriisilahenduskõlblikkuse hindamisel arvesse.

DORA määruses sätestatud mõiste „kriitilise tähtsusega või oluline funktsioon“ hõlmab direktiivi 2014/59/EL artikli 2 lõike 1 punktis 35 sätestatud kriitiliste funktsioonide määratlust. Seega on viidatud direktiivi kohaselt kriitiliseks funktsiooniks peetavad funktsioonid hõlmatud kriitilise tähtsusega funktsioonide määratusega DORA määruse tähenduses. FELS-is on kriitiline funktsioon defineeritud § 5 lõikes 2.

Kuna FELS § 2 lõike 3 kohaselt käsitatakse krediidiasutusena ka investeerimisühingut ja tema suhtes kohaldatakse kõike krediidiasutuse suhtes sätestatut, siis ka allolevaid selgitusi tuleks lugeda nii, et kõik, mis on öeldud krediidiasutuse kohta, käib ka investeerimisühingu kohta. Samuti on oluline juhtida tähelepanu asjaolule, et FI on FELS-i mõttes kriisilahendusasutus. Kui FI-l, kui järelevalveasutusel, on krediidiasutuse või investeerimisühingu kohta mingi teave tegelikult olemas, siis muudatuste kohaselt võib osutuda vajalikuks teavitada FI-d, kui kriisilahendusasutust, samuti teatud asjaoludest. FIS § 4 lõike 4 kohaselt tagab FI vajalikus ulatuses finantsjärelevalve ja kriisilahendusülesannete funktsiooni omavahelise sõltumatuse.

FELS § 2 lõike 2 muutmine (ei ole seotud DORA ülevõtmisega, seaduses parandatakse EL määruse nimetus õigeks). Euroopa Parlamendi ja Nõukogu määrusega (EL) 2019/2033, 27. november 2019, mis käsitleb investeerimisühingute suhtes kohaldatavaid usaldatavusnõudeid ning millega muudetakse määrusi (EL) nr 1093/2010, (EL) nr 575/2013, (EL) nr 600/2014 ja (EL) nr 806/2014, muudeti Euroopa Parlamendi ja nõukogu määruse (EL) nr 575/2013 pealkirja, mistõttu viiakse FELS-is olev viide määrusele kooskõlla selle õige nimetusega.

FELS § 11 lõike 1 punkti 16 muutmine. Muudetav paragrahv reguleerib, mida peab krediidiasutuse finantsseisundi taastamise kava sisaldama. Muudatusega täpsustatakse sõnastust, et kava peab sisaldama muu hulgas korda ja meetmeid, tagamaks võrgu- ja infosüsteemide pidev toimimine. Võrgu- ja infosüsteeme tuleks hallata vastavalt DORA määruses sätestatule.

Võrgu- ja infosüsteemid on defineeritud DORA määruse artikli 3 punktis 2 („võrgu- ja infosüsteem“ – direktiivi (EL) 2022/2555 artikli 6 punktis 1 määratletud võrgu- ja infosüsteem).

Viide on NIS2 direktiivi definitsioonile, mis omakorda määratleb, et võrgu- ja infosüsteem on (a) direktiivi (EL) 2018/1972 artikli 2 punktis 1 määratletud elektroonilise side võrk[28]; (b) seade või omavahel ühendatud või seotud seadmete rühm, millest vähemalt ühes toimub mõne programmi kohaselt digiandmete automaatne töötlemine, või (c) digiandmed, mida salvestatakse, töödeldakse, saadakse päringutega või edastatakse punktidega a ja b hõlmatud komponente kasutades nende töö, kasutamise, kaitsmise või hooldamise jaoks.

FELS § 28 lõike 5 täiendamine uute punktidega 14^1 ja 14^2. Lõige 5 kohustab krediidiasutust või temaga ühte konsolideerimisgruppi kuuluvat isikut abistama FI-d (nõudmisel) ja esitama talle teavet, mis on kriisilahenduskava koostamiseks ja rakendamiseks vajalik. Samas lõikes on loetelu teabest, mida FI võib nõuda. Muudatusettepanekuga täiendatakse loetelu ning FI nõudmisel tuleb esitada andmed ka kriitilise tähtsusega kolmandast isikust info- ja tehnoloogiateenuse osutajate kohta ning digitaalse tegevuskerksuse testi tulemused.

Kriitilise tähtsusega kolmandast isikust IKT teenuseosutaja on defineeritud DORA määruse artikli 3 punktis 23. Tegemis on IKT teenuseosutajaga, kes määratakse kriitilise tähtsusega kolmandast isikust IKT teenuseosutajaks vastavalt DORA määruse artiklile 31 (nt suured pilveteenuseosutajad jne).

FELS § 29 lõike 1 punktide 5 ja 8 muutmine. Paragrahv 29 reguleerib, mida peab kriisilahenduskava sisaldama.

Punkti 5 kohaselt peab kava sisaldama informatsiooni selle kohta, millised on võimalused kriitiliste funktsioonide ja põhiäriliinid õiguslikult ja majanduslikult teistest funktsioonidest eraldamiseks, et tagada krediidiasutuse maksejõuetuse korral tema tegevuse jätkumine. Muudatusega lisatakse, et kirjeldatut ei tuleks teha mitte ainult tegevuse jätkumise tagamiseks, vaid ka digitaalse tegevuskerksuse tagamiseks.

Punkti 8 kohaselt peab kava sisaldama informatsiooni süsteemide kirjelduse kohta. Muudatusega täpsustatakse, et sealhulgas DORA määruses sätestatud võrgu- ja infosüsteemide kirjelduse kohta.

FELS § 33 lõike 4 punkti 4 muutmine ja täiendamine uue punktiga 4^1. Paragrahv 33 reguleerib, mida võetakse arvesse krediidiasutuse ja konsolideerimisgrupi kriisilahenduskõlblikkuse hinnangu koostamisel.

Punktis 4 täpsustatakse, et kui hinnatakse krediidiasutuse teenuslepingute täielikult täitmisele pööratavust krediidiasutuse kriisilahendusmenetluse korral, siis on teenuslepingu all mõeldud ka info- ja kommunikatsioonitehnoloogia teenuse osutamisega seotud lepingut. Samuti on täpsustatud, et see leping peaks olema püsiv (ingl k *robust*).

Uue punkti 4^1 kohaselt tuleb kriisilahenduskõlblikkuse hinnangu koostamisel võtta arvesse kriitilisi funktsioone ja põhiäriliine toetavate võrgu- ja infosüsteemide digitaalsest tegevuskerksust. Selleks on abiks info- ja kommunikatsioonitehnoloogiaga seotud intsidentide

[28] „elektroonilise side võrk“ – ülekandesüsteemid, mis võivad, aga ei pruugi põhineda püsitaristul või kesksel juhtimisel, ja vajaduse korral lülitus- ja marsruutimisseadmed ning muud vahendid, sealhulgas võrguelemendid, mis ei ole aktiivsed, mis võimaldavad edastada signaale kaabli kaudu, raadio teel, optiliselt või muude elektromagnetiliste vahendite abil, kasutades sealhulgas satelliitvõrke, püsivõrke (ahel- ja pakettkommuteeritud võrgud, k.a internet) ja mobiilsidevõrke, elektrikaabelsüsteeme, kui neid kasutatakse signaalide edastamiseks, raadio- ja teleringhäälinguvõrke ja kaabeltelevisioonivõrke, olenemata sellest, millist teavet nende kaudu edastatakse;

aruanded ja digitaalse tegevuskerksuse testimise tulemused. Sõnastuses on kasutatud „kui see on asjakohane“ – kui pole tõsiseid intsidente, pole ka teavitusi, mida arvesse võtta.

Seaduse normitehniline märkus. Muudetakse seaduse normitehnilist märkust, lisades sinna viite DORA direktiivile.

3.2. Eelnõu § 2. Finantsinspektsiooni seaduse muutmine

FIS § 6 lõike 1 uus punkt 7^5. Kuigi finantsjärelevalve üheks osaks on alati olnud mh järelevalve seoses finantsasutuse operatsiooniriskide, infoturbe ja talitluspidevusega, täiendatakse FI ülesannete paragrahvi uue punktiga, rõhutamaks, et FI täidab mh ülesandeid seoses järelevalvega finantsasutuste digitaalse tegevuskerksuse nõuete täitmise üle. Samuti nähakse eelnõuga ette, et asjakohastel juhtudel teeb FI koostööd Eesti ja teiste liikmesriikide küberturvalisuse pädevate asutustega (vt ka selgitusi FIS uue § 47^{11} juures).

FIS § 46 uus lõige 10. Kuigi FI osaleb aktiivselt ESA-de töös ja vastav säte on ka FIS § 46 lõikes 2, kohustab DORA määruse artikli 32 lõige 5 selgesõnaliselt liikmesriiki määrama pädeva asutuse, kes kuulub EL tasandil järelevaatamise foorumisse. Sellest tuleb ka juhtivat järelevalveasutust teavitada.

Nimelt reguleerib DORA määrus mh järelevaatamist kriitilise tähtsusega kolmandast isikust IKT-teenuseosutajate üle. Järelevaatamise foorum hindab igal aastal ühiselt kõigi kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate järelevaatamise tulemusi ja leide ning edendab koordineerimismeetmeid, et suurendada finantsasutuste digitaalset tegevuskerksust, edendada IKT kontsentratsiooniriski käsitlemise parimaid tavasid ja uurida riskide valdkonnaülest ülekandumist leevendavaid tegureid.

Foorum on ESA-de ühiskomitee allkomitee ning sellesse kuulub mh iga liikmesriigi finantsjärelevalve asutusest üks kõrgetasemeline esindaja, kes on ühtlasi selle asutuse ehk Eesti puhul FI töötaja.

FIS § 47 lõike 12 muutmine (ei ole seotud DORA ülevõtmisega, seaduses parandatakse EL määruse nimetus õigeks)**.** Euroopa Parlamendi ja Nõukogu määrusega (EL) 2019/2033, 27. november 2019, mis käsitleb investeerimisühingute suhtes kohaldatavaid usaldatavusnõudeid ning millega muudetakse määrusi (EL) nr 1093/2010, (EL) nr 575/2013, (EL) nr 600/2014 ja (EL) nr 806/2014, muudeti Euroopa Parlamendi ja nõukogu määruse (EL) nr 575/2013 pealkirja, mistõttu viiakse FIS-is viide määrusele kooskõlla selle õige nimetusega.

FIS uus § 47^{11} reguleerib FI koostööd teiste asutustega küberturvalisuse valdkonnas.

Lõiked 1 ja 2. DORA määruse ja NIS2 direktiivi pädevad asutused peavad tegema koostööd.

Lõike 1 punkti 1 kohaselt peaks FI saama DORA määruse artikli 42 lõike 5 kohaselt (vabatahtlikult) konsulteerida NIS2 direktiivi pädeva asutusega, kui küsimuseks on, kas finantsasutus peaks ajutiselt osaliselt või täielikult peatama NIS2 direktiivi kohaldamisalasse kuuluva kriitilise tähtsusega kolmandast isikust IKT-teenuseosutaja osutatava teenuse kasutamise või kasutuselevõtu. Vajaduse korral saab ka nõuda, et finantsasutused lõpetaksid osaliselt või täielikult kriitilise tähtsusega kolmandast isikust IKT-teenuseosutajaga sõlmitud lepingud. Kuna selline kriitilise tähtsusega IKT-teenuseosutaja kuulub suure tõenäosusega mõne teise lepinguriigi NIS2 kohase järelevalve alla, on selle kohta ette nähtud ka eraldi **lõige 2**.

Punkt 2. DORA määruse pädeval asutustel (FI/EKP) peaks olema võimalik küsida tehnilist nõu NIS2 direktiivi kohaselt määratud või asutatud pädevatelt asutustelt (RIA) ning kehtestada koostöökokkulepe, mille eesmärk on tagada tõhusad ja kiired reageerimise koordineerimismehhanismid. Kokkulepetes võib muu hulgas kindlaks määrata järelevalve ja järelevaatamise koordineerimise menetlused seoses NIS2 direktiivi kohaldamisalasse jäävate elutähtsate või oluliste üksustega, kes on DORA määruse artikli 31 kohaselt määratud kriitilise tähtsusega kolmandast isikust IKT teenuseosutajateks, sealhulgas uurimiste ja kohapealsete kontrollide läbiviimiseks kooskõlas liikmesriigi õigusega. Samuti võib kokku leppida teabevahetuse toimumise viisi, mis hõlmab juurdepääsu DORA pädeva asutuse ja NIS 2 pädeva asutuse nõutud teabele.

NIS2 direktiivi põhjenduspunkt 25 selgitab ka, et valdkondlikes liidu õigusaktides, millega nähakse ette küberturvalisuse riskijuhtimismeetmed või teatamiskohustus, millel on NIS2 sätestatuga vähemalt samaväärne mõju, võiks ette näha, et nende õigusaktide kohased pädevad asutused kasutavad selliste meetmete või kohustustega seoses oma järelevalve- ja täitmise tagamise volitusi NIS2 kohaselt määratud pädevate asutuste abil. Asjaomased pädevad asutused võivad sel eesmärgil kehtestada koostöökorra. Sellises koostöökorras võiks muu hulgas täpsustada järelevalvetegevuse koordineerimise korra, sealhulgas liikmesriigi õiguse kohaste uurimiste ja kohapealsete kontrollide korra ning pädevate asutuste vahelise järelevalvet ja täitmise tagamist käsitleva asjakohase teabe vahetamise mehhanismi, sealhulgas juurdepääsu kübervaldkonda puudutavale teabele, mida pädevad asutused käesoleva direktiivi kohaselt taotlevad.

Punkt 3. Lisaks reguleerib pädevate asutuste koostööd NIS2 direktiivi artikkel 13, mis ütleb, et selleks et tagada pädevate asutuste, ühtsete kontaktpunktide ja CSIRTide ülesannete ja kohustuste tulemuslik täitmine, tagavad liikmesriigid nii suures ulatuses kui võimalik asjakohase koostöö nende kõnealuse liikmesriigi organite ning õiguskaitseasutuste, andmekaitseasutuste, määruste (EÜ) nr 300/2008 ja (EL) 2018/1139 kohaste riiklike asutuste, määruse (EL) nr 910/2014 kohaste järelevalveasutuste, määruse (EL) 2022/2554 (DORA) kohaste pädevate asutuste, direktiivi (EL) 2018/1972 kohaste riigi reguleerivate asutuste, direktiivi (EL) 2022/2557 kohaste pädevate asutuste ning muude valdkondlike liidu õigusaktide kohaste pädevate asutuste vahel. Koostöö hõlmab ka korrapäraselt teabe vahetamist, sealhulgas intsidentide ja küberohtude kohta.

Kuna CER direktiivi artikli 9 kohaselt on krediidiasustuse ja finantsturutaristute puhul CER pädevaks asutuseks DORA pädeva asutus, peab ka selle direktiivi kohaselt liikmesriik tagama, et ta teeb koostööd NIS2 pädeva asutusega, vahetades temaga teavet küsimustes, mis puudutavad elutähtsaid teenuseosutajaid mõjutavaid küberturvalisuse riske, küberohte ja -intsidente ning muid kui küberriske, -ohte ja -intsidente, sealhulgas seoses asjakohaste meetmetega, mille on võtnud NIS2 kohased pädevad asutused.

Punktis 4 tuuakse eraldi välja, et FI ja RIA teevad koostööd muu hulgas seoses finantsasutuste süvatestimisega. Süvatestimine on reguleeritud DORA määruse artiklites 26 ja 27. Võttes arvesse RIA küberkompetentsi, aitab kahe asutuse vaheline koostöö tagada, et testimised viiakse läbi nõuetekohaselt ja RIA on samuti kaasatud vastavatesse toimingutesse.

Lisaks on koostöö kontekstis asjakohane juhtida tähelepanu DORA määruse artikli 47 lõikele 1, mille kohaselt on pädeval asutusel õigus osaleda NIS2 direktiivi artikli 14 alusel loodud koostöörühma tegevuses seoses nende teemade ja küsimustega, mis on seotud pädeva asutuse järelevalvega finantsasutuse üle. Lisaks võib pädev asutus sama artikli lõike 2 kohaselt taotleda sellises koostöörühmas osalemist, kui selles arutatakse küsimusi seoses elutähtsa või olulise üksusega, kes osutab Eesti finantsasutustele IKT-teenuseid ning kes on ühtlasi DORA määruse

tähenduses kriitilise tähtsusega kolmandast isikust IKT teenuseosutaja. Tegemis on IKT teenuseosutajaga, kes määratakse kriitilise tähtsusega kolmandast isikust IKT teenuseosutajaks vastavalt DORA määruse artiklile 31.

Lõike 3 eesmärk on tagada, et oluliste krediidiasutuste teavitused tõsistest intsidentidest jõuaksid mh Eesti Pangale. DORA määruse artikli 19 lõike 6 punkt e kohaselt saab riik määrata, et lisaks punktides a–d nimetatud asutustele edastatakse tõsiste intsidentide teavitus ja raportid ka muudele liikmesriigi õiguse kohastele avaliku sektori asutustele. Seega, kui FI edastab oluliselt krediidiasutuselt laekunud teavituse Euroopa Keskpangale, edastab ta selle ühtlasi Eesti Pangale.

Lõige 4. Kuigi FI teeb koostööd ESA-de ja Euroopa Keskpangaga ning seda reguleerivad nii FIS kui ka asjakohased EL õigusaktid, on lõikes 6 täpsustatud, et koostöö hõlmab muu hulgas DORA määruse artiklite 48 ja 49 lõigetes 2 sätestatud koostööd ja teabevahetust. Artikli 48 lõike 2 kohaselt vahetavad pädevad asutused ja juhtiv järelevaatamisasutus (kelleks on üks ESA-dest, sõltuvalt, kes on kriitilise tähtsusega kolmandast isikust IKT teenuseosutaja) vahetavad aegsasti vastastikku kogu asjakohast teavet kriitilise tähtsusega kolmandast isikust IKT teenuseosutajate kohta, mida neil on vaja DORA määrusest tulenevate ülesannete täitmiseks, eelkõige seoses juhtiva järelevaatamisasutuse järelevaatamise ülesannete raames kindlaks tehtud riskide, lähenemisviiside ja võetud meetmetega.

Artikli 49 lõike 2 kohaselt teevad pädevad asutused, ESA-d ja Euroopa Keskpank omavahel tihedat koostööd ja vahetavad teavet, et täita oma DORA määruse artiklite 47–54 kohaseid ülesandeid. Nad kooskõlastavad tihedalt oma järelevalvetegevust, et teha kindlaks rikkumised ja võtta parandusmeetmeid, töötada välja ja edendada parimaid tavasid, hõlbustada koostööd, edendada tõlgendamise ühtsust ning anda lahkhelide korral jurisdiktsiooniüleseid hinnanguid.

FIS § 54 lõike 4 täiendamine uue punktiga. Paragrahv 54 reguleerib kontrollimisandmete salastatust. Lõikes 4 on loetelu asutustest, kellele konfidentsiaalse teabe ja finantsjärelevalve tulemusi kajastavate dokumentide avaldamine on lubatud. Lõiget täiendatakse uue punktiga, mille kohaselt on konfidentsiaalse teabe ja finantsjärelevalve tulemusi kajastavate dokumentide avaldamine lubatud RIA-le ulatuses, mis on vajalik tõhusaks koostööks kahe asutuse vahel. Siinjuures on oluline välja tuua, et ka DORA määruse 55 kohaselt kehtib DORA määruse alusel saadud, vahetatud või edastatud konfidentsiaalse teabe suhtes ametisalauduse hoidmise kohustus, sealhulgas teabevahetust DORA määruse pädevate asutuste (FI) ja NIS2 direktiivi kohaselt määratud või asutatud pädevate asutuste (RIA) vahel, ei avaldata ühelegi teisele isikule ega asutusele, välja arvatud juhul, kui see on ette nähtud liidu või liikmesriigi õigusega.

FIS § 54^4 uue lõikega 4^1 võetakse riigisisesesse õigusesse üle DORA määruse artikkel 56. Kuigi DORA määrus on otsekohalduv, on selle artiklis 53 sätestatud, et liikmesriigid teavitavad komisjoni, ESMA-t, EBA-t ja EIOPA-t oma õigus- ja haldusnormidest, millega võetakse üle peatükk 7 ehk ka viidatud peatükk tuleb riigisisesesse õigusesse üle võtta.

3.3. Eelnõu § 3. Hoiu-laenuühistute seaduse muutmine

Hoiu-laenuühistud kuuluvad vaikimisi DORA määruse kohaldamisalasse. Samas lubab DORA määruse artikli 2 lõige 4 riigisiseselt otsustada, et hoiu-laenuühistud ei kuulu DORA määruse kohaldamisalasse: „Liikmesriigid võivad käesoleva määruse kohaldamisalast välja arvata direktiivi 2013/36/EL artikli 2 lõike 5 punktides 4–23 osutatud üksused, mis asuvad nende vastaval territooriumil. Kui liikmesriik otsustab vastavale asutusele DORA määrust kohaldada, siis kohaldub neile IKT-riskide juhtimisraamistiku lihtsustatud režiim.“. Direktiivi 2013/36/EL artikli 2 lõike 5 punktis 6 on viidatud Eesti puhul hoiu-laenuühistutele, mis on hoiu-laenuühistu

seaduse kohaselt tunnustatavad ühistud. DORA määruse artikli 46 punkti a kohaselt oleks sellisel juhul pädevaks asutuseks sama asutus, kes on krediidiasutuste pädev asutus ehk Eesti puhul oleks selleks FI.

Kuna õiguslikult ei ole hoiu-laenuühistud hetkel FI finantsjärelevalve subjektid, on keeruline nende suhtes DORA määruse nõudeid kohaldada. Käesoleva eelnõuga samaaegselt on menetluses hoiu-laenuühistute seaduse ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu, mille lõplikust sisust sõltub, kuidas näha ette digitaalse tegevuskerksuse nõuete rakendamine ka hoiu-laenuühistutele.

Muudatusettepaneku kohaselt ei ole hoiu-laenuühistu kohustatud järgima DORA määruses sätestatud nõudeid.

3.4. Eelnõu § 4. Investeerimisfondide seaduse muutmine

IFS § 12 lõike 1 punkti 1 muutmine (ei ole seotud DORA ülevõtmisega, seaduses parandatakse EL määruse nimetus õigeks). Euroopa Parlamendi ja Nõukogu määrusega (EL) 2019/2033, 27. november 2019, mis käsitleb investeerimisühingute suhtes kohaldatavaid usaldatavusnõudeid ning millega muudetakse määrusi (EL) nr 1093/2010, (EL) nr 575/2013, (EL) nr 600/2014 ja (EL) nr 806/2014, muudeti Euroopa Parlamendi ja nõukogu määruse (EL) nr 575/2013 pealkirja, mistõttu viiakse IFS-is viide määrusele kooskõlla selle õige nimetusega.

IFS § 223 lõike 2 muutmine. DORA määruse kohaldamisse kuuluvad mh määratud väljamaksetega tööandja pensionifondid (IORP-id). Paragrahvis 223 on viited IFS paragrahvidele, milledes sätestatut peab ka IORP oma tegevuses arvestama. Muudatusega lisatakse §-i 223 viide IFS §-le 345, mille uus lõige 1^1 kohustab fondivalitsejaid järgima DORA määruses sätestatut. Lisaks on viide IFS uuele §-le 345^1 ehk ka IORP-ide puhul on kohustus teavitada nii FI-d kui ka RIA-t tõsistest info- ja kommunikatsioonitehnoloogiaga seotud intsidentidest ning soovi korral olulistest küberohtudest.

IFS § 223 uus lõige 5. Proportsionaalsuse põhimõtte kohaselt ei kohaldata DORA määrust IORP-ide suhtes, milles on vähem kui 15 pensioniskeemiga hõlmatud isikut.

IFS § 344 lõike 3 punkti 3 muutmine. Fondivalitseja sise-eeskirjade puhul täpsustatakse, et nõuded info- ja kommunikatsioonitehnoloogilise korralduse, infoturbe tagamise ja talitluspidevuse kohta tuleb asjakohasel juhul koostada kooskõlas DORA määruses sätestatud info- ja kommunikatsiooniriskide juhtimise raamistikuga. Kuna DORA määrus ei kohaldu IORP-ide suhtes, millesse kuulub vähem kui 15 pensioniskeemiga hõlmatud isikut, on õigusselguse huvides sõnastuses täpsustatud „asjakohasel juhul“, ehk jättes DORA-le viite kohustusest välja kõnealused IORP-id. Samas pensionifondi valitsejate puhul peavad sise-eeskirjad info- ja kommunikatsioonitehnoloogilise korralduse, infoturbe tagamise ja talitluspidevuse kohta olema koostatud kooskõlas DORA määrusega (vt selgitust ka IFS § 345 lõike 1^1 juures).

IFS § 345 pealkirja muutmine. Kuna paragrahvi sisu täiendatakse viitega DORA määrusele, siis viiakse ka pealkiri kooskõlla selle sisuga.

IFS § 345 uus lõige 1^1. Kuna fondivalitsejad kuuluvad samuti DORA kohaldamisalasse, on §-i 345 lisatud kohustus järgida DORA määruses sätestatud nõudeid, sealjuures peavad loodavad ja hallatavad võrgu- ja infosüsteemid vastama DORA määruses sätestatule.

Pensionifondide puhul ei ole tegemist eurofondi valitsejaga direktiivi 2009/65/EÜ artikli 2 lõike 1 punkti b tähenduses, mistõttu ei kuulu nad vaikimisi ka DORA määruse kohaldamisalasse. Eelnõu koostamisel on võetud lähenemine, et ka pensionifondid lähtuvad oma tegevuses DORA määruses sätestatud nõuetest, mistõttu on õigusselguse huvides sõnastuses ka nendele eraldi viidatud. Samas on täpsustatud, et mitte kõikide DORA määruse sätete puhul ei ole kohane määrust pensionifondi valitseja suhtes kohaldada. Nimelt ei saa nende suhtes kohaldada neid sätteid, mis on seotud teiste Euroopa institutsioonide tegevusega. Näiteks ei saa kohustada FI-d saatma pensionifondi valitseja edastatud teated intsidentide kohta edasi ESA-dele, kuna nendega seotud järelevalve ei kuulu Euroopa finantsjärelevalve süsteemi. Samuti ei saa kriitiliste IKT teenuseosutajate järelevaatamise puhul arvesse võtta olukordi, kus nad osutavad teenust pensionifondi valitsejatele.

Järgnevalt on esitatud ülevaade pensionifondi valitsejale kohalduvatest kehtivatest IKT ja küberturvalisuse nõuetest/suunistest ning DORA kohaldumisel kohalduvatest nõuetest. Oluline on siinjuures märkida, et DORA määruse muutmisel tuleb kohaldatavad sätted pensionifondi valitsejate vaates uuesti riigisiseselt läbi analüüsida, et tagada, et ka muudatuste korral on neid asjakohane kohaldada pensionifondi valitsejatele.

Kehtiv	Uus
IKT riskijuhtimisraamistik (II peatükk)	
§ IFS 344 lg 3 p 3: Sise-eeskirjadega määratakse: - nõuded infotehnoloogilise korralduse, infoturbe tagamise ja talitluspidevuse kohta. Finantsinspektsiooni soovituslikud juhendid: - Nõuded finantsjärelevalve subjekti infotehnoloogia ja infoturbe korraldusele; - Nõuded finantsjärelevalve subjekti talitluspidevuse protsessi korraldamiseks.	- nõuded info- ja kommunikatsioonitehnoloogilise korralduse, infoturbe tagamise ja talitluspidevuse kohta, mis peavad asjakohasel juhul olema kooskõlas Euroopa Parlamendi ja nõukogu määruses (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 (ELT L 333, 27.12.2022, lk 1–79), sätestatud info- ja kommunikatsioonitehnoloogia riskide juhtimise raamistikuga.
	- IFS § 345 (1^1). Pensionifondi valitseja suhtes kohaldatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2022/2554 artiklites 3–18, artikli 19 lõigetes 1–5, artikli 22 lõikes 1, artiklites 24–30 ning artiklis 45 sätestatut.“;
IKT intsidentide haldamine ja liigitamine ning nendest teavitamine (III peatükk)	
Finantsinspektsiooni soovituslik juhend: - Nõuded finantsjärelevalve subjekti infotehnoloogia ja infoturbe korraldusele.	IFS § 345 (1^1). DORA määruse artiklid 17 ja 18, artikli 19 lõiked 1–5 ning artikli 21 lõige 1.
Digitaalse tegevuskerksuse testimine (IV peatükk)	
Finantsinspektsiooni soovituslik juhend: - Nõuded finantsjärelevalve subjekti infotehnoloogia ja infoturbe korraldusele;	IFS § 345 (1^1), artiklid 24–27.

- Nõuded finantsjärelevalve subjekti talitluspidevuse protsessi korraldamiseks.	
Kolmandast isikust tuleneva IKT-riski juhtimine (V peatüki I jagu)	
Finantsinspektsiooni soovituslikud juhendid: - Nõuded finantsjärelevalve subjekti infotehnoloogia ja infoturbe korraldusele. - Nõuded finantsjärelevalve subjekti poolt tegevuse edasiandmisele (Outsourcing).	IFS § 345 (1^1), DORA määruse artiklid 28–30.
Teabe jagamise kokkulepped (VI peatükk)	
-	IFS § 345 (1^1), DORA määruse artikkel 45.

Selguse huvides tasub ka välja tuua, et uued digitaalse tegevuskerksuse nõuded ei kohaldu IFS § 3 lõikes 6 määratletud väikefondi valitsejatele.

IFS uus § 345[1]. DORA määruse artikli 19 lõike 1 kohaselt peab finantsasutus teavitama pädevat asutust tõsistest IKT-ga seotud intsidentidest. Lisaks annab määrus liikmesriigile võimaluse ette näha, et mõned või kõik finantssektori ettevõtjad esitavad pädevale asutusele või küberturbe intsidentide lahendamise üksustele, mis on määratud või loodud direktiivi (EL) 2022/2555 kohaselt, samuti esialgse teate ja kõik raportid, kasutades DORA määruse artiklis 20 osutatud teavitusvorme (**lõiked 1 ja 2**). Lõikega 1 nähakse ette, et fondivalitseja teavitab lisaks FI-le ka RIA-t.

Intsidentide liigitamise kriteeriumid on ette nähtud DORA määruse artikli 18 lõikes 1, kuid täpsemad kriteeriumid tõsiste intsidentide määratlemiseks töötavad välja ESA-d koostöös EKP ja ENISA-ga.

Lisaks sätestab DORA määruse artikli 19 lõige 2, et finantsasutused võivad vabatahtlikult teatada asjaomasele pädevale asutusele olulistest küberohtudest, kui nad peavad ohtu finantssüsteemi, teenusekasutajate või klientide jaoks oluliseks, sealjuures võivad liikmesriigid otsustada, et need finantsasutused, kes teatavad vabatahtlikult esimese lõigu kohaselt, võivad kõnealuse teate edastada ka direktiivi (EL) 2022/2555 kohaselt määratud või loodud küberturbe intsidentide lahendamise üksustele.

IFS § 363[1] uus lõige 3. Selguse huvides on ka tööandja pensionifondide puhul välja toodud, et DORA määrust ei kohaldata sellise fondivalitseja suhtes, kes valitseb fondi, milles on vähem kui 15 (sh) osakuomanikku.

IFS § 455 uus lõige 3[2]. Paragrahv reguleerib järelevalve aluseid ja kohaldamist. Eelnõuga lisatakse paragrahvi uus lõige, milles sätestatakse, et FI-l on õigus rakendada DORA määruse artiklis 50 sätestatud õigusi ja meetmeid ning FI avalikustab vastavate meetmete alusel tehtud otsuse kohta teate oma veebilehel, nagu on sätestatud DORA määruse artiklis 54.

Näiteks on FI-l õigus tutvuda kõigi dokumentidega või mis tahes vormis muude andmetega, mis võiksid olla FI ülesannete täitmiseks olulised, ja saada või teha nende dokumentide koopiaid, teha kohapealseid kontrolle või uurimisi ning nõuda määruse nõuete rikkumise korral parandus- ja ennetusmeetmete võtmist.

DORA määruse artikli 50 lõige 4 kohustab liikmesriike pädevatele asutustele andma õiguse kohaldada määruse nõuete rikkumise korral halduskaristusi või parandusmeetmeid. Sellisteks meetmeteks on:

- ettekirjutuse tegemine, et füüsiline või juriidiline isik lõpetaks rikkuva tegevuse ja hoiduks selle tegevuse kordamisest;
- sellise tegevuse või tava peatamise nõudmine, mis on vastuolus määruse sätetega;
- mis tahes liiki meetmete võtmine, sealhulgas rahaliste meetmete, tagamaks, et finantsasutused jätkavad õigusnormide järgimist;
- liikmesriigi õigusega lubatud ulatuses sideoperaatorite valduses olete andmeliiklusandmete nõudmine, kui on piisav alus kahtlustada määruse nõuete rikkumist ja kui sellised andmed võivad olla olulised määruse rikkumiste uurimisel, ning
- avalike teadaannete väljastamine, mis sisaldavad füüsilise või juriidilise isiku identiteeti ja rikkumise laadi.

Et võetud meetmetel oleks hoiatav mõju laiemale avalikkusele, näeb määrus ette rikkumist puudutavate otsuste ja rakendatud meetmete avalikustamise. DORA määruse artikli 54 lõike 1 kohaselt avaldavad pädevad asutused oma ametlikel veebisaitidel põhjendamatu viivituseta kõik halduskaristuse määramise otsused, mida ei ole edasi kaevatud pärast seda, kui karistuse saanud isikut on otsusest teavitatud. Avaldada tuleb teave rikkumise liigi ja laadi kohta, vastutavad isikud ning määratud karistused. Erandiks on olukorrad, kus juriidilise isiku nime või füüsilise isiku nime ja isikuandmete avaldamine oleksid ebaproportsionaalsed või nende andmete avaldamine ohustaks finantsturgude stabiilsust või pooleli olevat uurimist (eelkõige mõeldud järelevalve- ja väärteomenetlust, kuid võib hõlmata ka kriminaalmenetlust tegevusloata tegutsemise puhul) või põhjustaks asjaomasele isikule ebaproportsionaalselt suurt kahju. Sellisel puhul võib avaldamise edasi lükata, jätta isikuid puudutav teave avaldamata või loobuda sellise kaasuse kohta teabe avaldamisest üldse.

IFS uus § 503[4]. Seadust täiendatakse uue karistusnormiga, mida FI saab rakendada DORA määruses sätestatud nõuete rikkumise korral. Nimelt on DORA määruse artikli 50 lõikes 3 sätestatud, et liikmesriigid kehtestavad õigusnormid, milles sätestatakse asjakohased halduskaristused ja parandusmeetmed määruse rikkumise puhuks, ning tagavad nende tulemusliku rakendamise. Sama artikli lõike 4 punktis c on sätestatud, et liikmesriigid annavad pädevatele asutustele õiguse võtta mis tahes liiki meetmeid, sealhulgas rahalisi meetmeid, tagamaks, et finantssektori ettevõtjad jätkavad õigusnormide järgimist. Eelnõuga nähakse ette, et füüsilise isiku korral on võimalik karistada rahatrahviga kuni 5 000 000 eurot või kuni kahekordse väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas ning juriidilise isiku korral karistatakse rahatrahviga kuni 5 000 000 eurot või kuni kahekordse väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas või kuni kümme protsenti juriidilise isiku või tema konsolideerimisgrupi konsolideeritud käibest.

Uue paragrahvi lõike 1 sõnastuses on viidatud järgmistele DORA määruse nõuete rikkumistele:
- art 5–14: IKT- riski juhtimine;
- art 16–18, art 19 lõiked 1–5: IKT intsidentide haldamine ja liigitamine ning nendest teavitamine;
- art 24, 25, art 27 lõiked 1–8: digitaalse tegevuskerksuse testimine;
- art 28 lõiked 1–8, art 29, art 30 lõiked 1–4: kolmandast isikust tuleneva IKT-riski juhtimine;
- art 42 lg 3: kolmanda isikuga seotud riskide arvesse võtmine.

Seaduse normitehniline märkus. Muudatusega lisatakse viide DORA direktiivile.

3.5. Eelnõu § 5. Kindlustustegevuse seaduse muutmine

Direktiiv 2009/138/EÜ käsitleb IKT-riski teataval määral üldjuhtimise ja riskijuhtimise üldsätetes, jättes teatavate nõuete täpsustamise delegeeritud õigusaktide ülesandeks, mitte alati

viidates selleks konkreetselt IKT-riskile. Kuna viidatud direktiiv viiakse kooskõlla DORA määrusega, peegelduvad vastavad muudatused ka KindlTS-is.

KindlTS § 38 lõike 2 punkt 5 ja uus punkt 5[1] (ei ole seotud DORA direktiiviga, kuid on tehniline muudatus, et vältida seaduses olevat tühja viidet). Kuna ÄS § 386 lõike 2 punkt 4 on tunnistatud kehtetuks, korrigeeritakse KindlTS sõnastust ja kustutatakse viide kehtetule ÄS punktile 4. ÄS-ist välja jäetud punkt sõnastatakse KindlTS-is. Seega peab kolmanda riigi kindlustusandja Eestis filiaali asutamise loa taotlemisel esitama FI-le äriühingu põhikirja või ühingulepingu asukohamaa seaduste kohaselt tõestatud ärakirja, kui põhikirja või ühingulepingu registrile esitamine on nõutav ka ühingu asukohamaal.

KindlTS § 87 lõike 9 muutmine (ei ole seotud DORA direktiiviga, kuid seaduses parandatakse EL määruse nimetus õigeks). Euroopa Parlamendi ja Nõukogu määrusega (EL) 2019/2033, 27. november 2019, mis käsitleb investeerimisühingute suhtes kohaldatavaid usaldatavusnõudeid ning millega muudetakse määrusi (EL) nr 1093/2010, (EL) nr 575/2013, (EL) nr 600/2014 ja (EL) nr 806/2014, muudeti Euroopa Parlamendi ja nõukogu määruse (EL) nr 575/2013 pealkirja, mistõttu viiakse KindlTS-is viide määrusele kooskõlla selle õige nimega.

KindlTS § 96 täiendamine uue lõikega 7[1]. Kindlustusandja juhtimissüsteemi nõuete hulka kuulub ka DORA määruse rakendamine. Sealhulgas peab kidnlustusandja kasutama ja haldama info- ja võrgusüsteeme vastavalt DORA määruses sätestatule.

KindlTS § 105 muutmine. Kindlustusandja sise-eeskirjade puhul täpsustatakse, et nõuded info- ja kommunikatsioonitehnoloogilise korralduse, infoturbe tagamise ja talitluspidevuse kohta tuleb koostada kooskõlas DORA määruses sätestatud info- ja kommunikatsiooniriskide juhtimise raamistikuga.

KindlTS uus § 105[1]. DORA määruse artikli 19 lõike 1 kohaselt peab finantsasutus teavitama pädevat asutust tõsistest IKT-ga seotud intsidentidest. Lisaks annab määrus liikmesriigile võimaluse ette näha, et mõned või kõik finantssektori ettevõtjad esitavad pädevale asutusele või küberturbe intsidentide lahendamise üksustele, mis on määratud või loodud direktiivi (EL) 2022/2555 kohaselt, ka esialgse teate ja kõik raportid, kasutades DORA määruse artiklis 20 osutatud vorme (**lõiked 1 ja 2**). Lõikega 1 nähakse ette, et kindlustusandja teavitab lisaks FI-le ka RIA-t.

Intsidentide liigitamise kriteeriumid on ette nähtud DORA määruse artikli 18 lõikes 1, kuid täpsemad kriteeriumid tõsiste intsidentide määratlemiseks töötavad välja ESA-d koostöös EKP ja ENISA-ga.

Lisaks sätestab DORA määruse artikli 19 lõige 2, et finantsasutused võivad vabatahtlikult teatada asjaomasele pädevale asutusele olulistest küberohtudest, kui nad peavad ohtu finantssüsteemi, teenusekasutajate või klientide jaoks oluliseks, sealjuures võivad liikmesriigid otsustada, et need finantsasutused, kes teatavad vabatahtlikult esimese lõigu kohaselt, võivad kõnealuse teate edastada ka direktiivi (EL) 2022/2555 kohaselt määratud või loodud küberturbe intsidentide lahendamise üksustele (**lõige 3**).

KindlTS § 138 muutmine (ei ole seotud DORA direktiiviga)**.** Paragrahvi lisatakse uus lõige, mille kohaselt ei ole kindlustusandjate piiriülene ümberkujundamine lubatud. Piiriülene ümberkujundamine tähendab, et Eesti äriühingu saab ümber kujundada lepinguriigi äriühinguks. Arvestades, et finantssektoris teenuse osutamiseks peab isikul olema tegevusluba, mille ta saab asukoha finantsjärelevalve asutuselt, ei ole tarbijakaitse seisukohast asjakohane olukord, kus kindlustusandja viib tegevuse ja kindlustusportfelli üle teise lepinguriiki, kus tal

puudub vastava lepinguriigi finantsjärelevalve asutuse luba selles riigis kindlustusteenuse osutamiseks. Samas ei ole tal võimalik tegevusluba taotleda, kui ta on alles Eesti registrisse kuuluv äriühing. Seega kindlustusvõtjate ja kindlustatute kaitse seisukohast ei ole võimalik tagada, et piiriülese ümberkujundamise korral oleks viidatud isikute huvid piisavalt kaitstud. Alternatiiv on asutada lepinguriigis uus kindlustusandja, kellega Eesti kindlustusandja ühineb või kellele Eesti kindlustusandja annab kindlustusportfelli üle. Sellisteks olukordadeks on KindlTS ette nähtud ka vastav regulatsioon klientide kaitseks.

Euroopa Parlamendi ja Nõukogu Direktiiv (EL) 2019/2121, millega muudetakse direktiivi (EL) 2017/1132 seoses äriühingute piiriülese ümberkujundamise, ühinemise ja jagunemisega põhjenduspunkti 57 kohaselt ei tohiks viidatud direktiiv mõjutada liidu õiguse kohaldamist, mis reguleerib krediidivahendusettevõtjaid ja teisi finantsettevõtjaid, ega vastavalt kõnealusele liidu õigusele kehtestatud liikmesriigi õigusnormide kohaldamist. Kindlustustegevust reguleeriva Euroopa Parlamendi ja nõukogu direktiivi 2009/138/EÜ peaeesmärk on kindlustusvõtjate ja soodustatud isikute asjakohane kaitse (põhjenduspunkt 14). Seega on kindlustusandjate piiriülese ümberkujundamise piirang kooskõlas eelnimetatud direktiivi põhimõttega, et tagada tuleb kindlustusvõtjate ja soodustatud isikute kaitse.

KindlTS § 175 lõike 1 muutmine. Kuna DORA määrus kohaldub ka kindlustusvahendajatele, sealhulgas §-s 175 defineeritud kõrvalvahendajatele, on § 175 lõikesse 1 lisatud viide uuele §-le 181^1, milles reguleeritakse, et kindlustusvahendajatele kohalduvad digitaalse tegevuskerksuse nõudeid.

KindlTS uus § 181^1. DORA määrus kohaldub nii kindlustusmaakleritele kui ka kindlustusagentidele (**lõige 1**), samas on siinjuures oluline asjaolu, et määrust ei pea rakendama mikroettevõtjast ning väikese ja keskmise suurusega kindlustusvahendajad. Seega, kui ettevõtjas töötab vähem kui 250 inimest ja selle ettevõtja aastakäive ei ületa 50 miljonit eurot ja/või aastabilanss ei ületa 43 miljonit eurot, siis määrus sellele vahendajale ei kohaldu (**lõige 3**).

Lõikes 2 sätestatakse, et tõsistest IKT intsidentidest ja küberohtudest teavitamisele kohaldatakse §-s 105^1 sätestatut, kindlustusvahendajad peavad teavitama nii FI-d kui ka RIA-t tõsistest IKT-ga seotud intsidentidest.

KindlTS § 186 lõike 2 punkti 13 muutmine. Kindlustusmaakleri sise-eeskirjade puhul täpsustatakse, et kui kindlustusmaaklerile kohaldub DORA määrus (sõnastuses kasutatud „asjakohasel juhul"), siis nõuded info- ja kommunikatsioonitehnoloogilise korralduse, infoturbe tagamise ja talitluspidevuse kohta peaksid olema koostatud kooskõlas DORA määruses sätestatud IKT riskijuhtimise raamistikuga. Kuna üldjuhul Eesti kindlustusvahendajad ei kuulu oma suuruse tõttu DORA kohaldamisalasse, on oluline, et ka neile jääks siiski kohustus kehtestada sise-eeskirjaga nõuded tehnoloogilise korralduse, infoturbe tagamise ja talitluspidevuse kohta.

KindlTS § 210 lõike 1 punkt 4 (ei ole seotud DORA direktiiviga, kuid on tehniline muudatus, et vältida seaduses olevat tühja viidet). Kuna ÄS § 386 lõike 2 punkt 4 on tunnistatud kehtetuks, korrigeeritakse KindlTS sõnastust ja kustutatakse viide kehtetule ÄS punktile 4. ÄS-ist välja jäetud punkt sõnastatakse KindlTS-is. Seega peab kolmanda riigi kindlustusvahendaja Eestis filiaali asutamise loa taotlemisel esitama FI-le äriühingu põhikirja või ühingulepingu asukohamaa seaduste kohaselt tõestatud ärakirja, kui põhikirja või ühingulepingu registrile esitamine on nõutav ka ühingu asukohamaal.

KindlTS § 224 uus lõige 3. Paragrahv reguleerib järelevalve ülesandeid ja õigusi. Eelnõuga lisatakse paragrahvi uus lõige, milles sätestatakse, et FI-l on õigus rakendada DORA määruse artiklis 50 sätestatud õigusi ja meetmeid ning FI avalikustab vastavate meetmete alusel tehtud otsuse kohta teate oma veebilehel nagu on sätestatud artiklis 54.

Näiteks on FI-l õigus tutvuda kõigi dokumentidega või mis tahes vormis muude andmetega, mis võiksid olla FI ülesannete täitmiseks olulised, ja saada või teha nende dokumentide koopiaid, teha kohapealsed kontrolle või uurimisi ning nõuda määruse nõuete rikkumise korral parandus- ja ennetusmeetmete võtmist.

DORA määruse artikli 50 lõige 4 kohustab liikmesriike pädevatele asutustele andma õiguse kohaldada määruse nõuete rikkumise korral halduskaristusi või parandusmeetmeid. Sellisteks meetmeteks on:
- ettekirjutuse tegemine, et füüsiline või juriidiline isik lõpetaks rikkuva tegevuse ja hoiduks selle tegevuse kordamisest;
- sellise tegevuse või tava peatamise nõudmine, mis on vastuolus määruse sätetega;
- mis tahes liiki meetmete võtmine, sealhulgas rahaliste meetmete, tagamaks, et finantsasutused jätkavad õigusnormide järgimist;
- liikmesriigi õigusega lubatud ulatuses sideoperaatorite valduses olete andmeliiklusandmete nõudmine, kui on piisav alus kahtlustada määruse nõuete rikkumist ja kui sellised andmed võivad olla olulised määruse rikkumiste uurimisel, ning
- avalike teadaannete väljastamine, mis sisaldavad füüsilise või juriidilise isiku identiteeti ja rikkumise laadi.

Et võetud meetmetel oleks hoiatav mõju laiemale avalikkusele, näeb määrus ette rikkumist puudutavate otsuste ja rakendatud meetmete avalikustamise. DORA määruse artikli 54 lõike 1 kohaselt avaldavad pädevad asutused oma ametlikel veebisaitidel põhjendamatu viivituseta kõik halduskaristuse määramise otsused, mida ei ole edasi kaevatud pärast seda, kui karistuse saanud isikut on otsusest teavitatud. Avaldada tuleb teave rikkumise liigi ja laadi kohta, vastutavad isikud ning määratud karistused. Erandiks on olukorrad, kus juriidilise isiku nime või füüsilise isiku nime ja isikuandmete avaldamine oleksid ebaproportsionaalsed või nende andmete avaldamine ohustaks finantsturgude stabiilsust või pooleli olevat uurimist (eelkõige mõeldud järelevalve- ja väärteomenetlust, kuid võib hõlmata ka kriminaalmenetlust tegevusloata tegutsemise puhul) või põhjustaks asjaomasele isikule ebaproportsionaalselt suurt kahju. Sellisel puhul võib avaldamise edasi lükata, jätta isikuid puudutav teave avaldamata või loobuda sellise kaasuse kohta teabe avaldamisest üldse.

KindlTS uus § 257[1]. Seadust täiendatakse uue karistusnormiga, mida FI saab kohaldada DORA määruses sätestatud nõuete rikkumise korral. Nimelt on DORA määruse artikli 50 lõikes 3 sätestatud, et liikmesriigid kehtestavad õigusnormid, milles sätestatakse asjakohased halduskaristused ja parandusmeetmed määruse rikkumise puhuks, ning tagavad nende tulemusliku rakendamise. Sama artikli lõike 4 punktis c on sätestatud, et liikmesriigid annavad pädevatele asutustele õiguse võtta mis tahes liiki meetmeid, sealhulgas rahalisi meetmeid, tagamaks, et finantssektori ettevõtjad jätkavad õigusnormide järgimist. Eelnõuga nähakse ette, et füüsilise isiku korral on võimalik karistada rahatrahviga kuni 5 000 000 eurot või kuni kahekordse väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas ning juriidilise isiku korral karistatakse rahatrahviga kuni 5 000 000 eurot või kuni kahekordse väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas või kuni kümme protsenti juriidilise isiku või tema konsolideerimisgrupi konsolideeritud käibest.

Uue paragrahvi lõike 1 sõnastuses on viidatud järgmistele DORA määruse nõuete rikkumistele:
- art 5–14: IKT- riski juhtimine;

- art 16–18, art 19 lõiked 1–5: IKT intsidentide haldamine ja liigitamine ning nendest teavitamine;
- art 24, 25, art 27 lõiked 1–8: digitaalse tegevuskerksuse testimine;
- art 28 lõiked 1–8, art 29, art 30 lõiked 1–4: kolmandast isikust tuleneva IKT-riski juhtimine;
- art 42 lg 3: kolmanda isikuga seotud riskide arvesse võtmine.

Seaduse normitehniline märkus. Muudatusega lisatakse viide DORA direktiivile.

3.6. Eelnõu § 6. Krediidiandjate ja -vahendajate seadus

KAVS § 28 lõike 5 muutmine (ei ole seotud DORA direktiiviga, seaduses parandatakse EL määruse nimetus õigeks)**.** Euroopa Parlamendi ja Nõukogu määrusega (EL) 2019/2033, 27. november 2019, mis käsitleb investeerimisühingute suhtes kohaldatavaid usaldatavusnõudeid ning millega muudetakse määrusi (EL) nr 1093/2010, (EL) nr 575/2013, (EL) nr 600/2014 ja (EL) nr 806/2014, muudeti Euroopa Parlamendi ja nõukogu määruse (EL) nr 575/2013 pealkirja, mistõttu viiakse KAVSis olev viide määrusele kooskõlla selle õige nimega.

KAVS § 61 uus lõige (ei ole seotud DORA direktiiviga). Muudatuse eesmärk on piirata krediidiandjate ja -vahendajate piiriülest ümberkujundamist, et tagada Eesti klientide parem kaitse. Arvestades finantssektori erisusi, ei ole praktikas krediidiandja ümberkujundamine võrreldav nn tavalise äriühingu ümberkujundamise protsessiga. Krediidiandja puhul peavad olema kaitstud klientide huvid, kuid piiriülese ümberkujundamise käigus võivad klientide huvid saada kahjustada, eelkõige olukorras, kus lepinguriigi krediidiandja ei kuulu järelevalve alla. Krediidiandjate ja -vahendajate regulatsioonid ei ole Euroopaüleselt sarnased ning puudub ühtlustatud „passport“ süsteem. Piiriülese ümberkujundamise korral viiakse kõik krediidiandja ja -vahendaja tarbijakrediidilepingud teise lepinguriiki, kus on erinev tarbijakaitse tase ja krediidiandjatele ja -vahendajatele kehtestatud regulatsioon.

Krediidiandjate ja -vahendajate piiriülene liikumine oli aruteluks 14.11.2022 Riigikogu õiguskomisjoni istungil[29], kus FI tutvustas võimalikke riske krediidiandjate ja -vahendajate piiriülese ümberkujundamise korral. Komisjoni ettepanek oli, et „Justiitsministeerium koos Rahandusministeeriumiga võiksid selle murekoha lahendamist arutada“.

3.7. Eelnõu § 7. Krediidiasutuste seaduse muutmine

Pangandusvaldkonna direktiivis 2013/36/EL on sätestatud üldised sisejuhtimise reeglid ja operatsiooniriski käsitlevad sätted, mis sisaldavad nõudeid situatsiooni- ja talitluspidevuse kavadele, mille alusel kaudselt käsitletakse IKT-riski. Selleks, et käsitleda IKT-riski ühemõtteliselt ja selgelt, muudetakse situatsiooni- ja talitluspidevuse plaanide nõudeid, et need hõlmaksid kooskõlas DORA määrusega ka IKT-riskiga seotud talitluspidevuse plaane ning reageerimis- ja taasteplaane.

Lisaks, selleks et tagada õigusselgus ning et pankade järelevalveasutused teeksid tulemuslikult kindlaks ja jälgiksid IKT-riski juhtimist kooskõlas digitaalse tegevuskerksuse uue raamistikuga, muudetakse järelevalvealase läbivaatamise ja hindamise protsessi kohaldamisala. Eesmärk on katta ka riske, mis tuuakse välja IKTga seotud tõsiseid intsidente puudutavates aruannetes ning mis on ilmnenud panga poolt DORA määruse alusel läbi viidud digitaalse tegevuskerksuse testimise käigus.

[29] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/75cf6d3f-bcfe-436e-bd51-3a1333c185ad/%C3%84riseadustiku+muutmise+ja+sellega+seonduvalt+teiste+seaduste+muutmise+seadus+%28%C3%A4ri%C3%BChingute+piiri%C3%BClene+liikumine%29/

KAS § 20[6] lõike 3 täpsustamine (ei ole seotud DORA direktiiviga)**.** Kuna kolmanda riigi krediidiasutus saab Eestis teenust osutada vaid filiaali kaudu, on selguse huvides täpsustatud, et filiaal peaks olema kantud ka Eestis äriregistrisse. Ehk kui ÄS § 384 lõige 1 ütleb, et välismaa äriühing võib filiaali kanda äriregistrisse, siis kolmanda riigi krediidiasutuste puhul tuleb filiaal äriregistrisse kanda, kuna piiriülene teenuse osutamine filiaali asutamata/registreerimata ei ole kolmanda riigi krediidiasutuse poolt lubatud. ÄS § 384 lõike 1 muudatust on selgitatud[30] järgmiselt: „Filiaali registreerimise kohustuse kaotamise eesmärgiks on muuta filiaali kaudu tegutsemine Eestis vabatahtlikuks. Kui välismaa äriühing soovib täiendavalt oma tegevuse Eesti nähtavaks teha, et tema andmed oleks Eesti äriregistris kättesaadavad, on võimalus filiaal Eesti äriregistris registreerida. See ei ole siiski ainuke võimalus välismaa äriühingule Eestis tegutsemiseks. Välismaa äriühing võib tegutseda Eestis piiriüleselt ka nii, et Eesti äriregistris filiaali ei registreeri. Seetõttu ei saa tekkida küsimust, kas on võimalik tegutseda ka registreerimata filiaali kaudu ja millised on nõuded registreerimata filiaalile. Kui välismaa äriühing ei ole äriregistris filiaali registreerinud, siis ei saa tema tegevust Eestis nimetada filiaali kaudu tegutsemiseks, vaid nimetatakse välismaa äriühingu piiriüleseks tegevuseks.“.

KAS § 21 lõike 2 punkti 5 muutmine ja uus punkt 6 (ei ole seotud DORA direktiiviga, kuid on tehniline muudatus, et vältida seaduses olevat tühja viidet). Kuna ÄS § 386 lõike 2 punkt 4 on tunnistatud kehtetuks, korrigeeritakse KAS sõnastust ja kustutatakse viide kehtetule ÄS punktile 4. ÄS-ist välja jäetud punkt sõnastatakse KAS-is. Seega peab kolmanda riigi krediidiasutus Eestis filiaali asutamise loa taotlemisel esitama FI-le äriühingu põhikirja või ühingulepingu asukohamaa seaduste kohaselt tõestatud ärakirja, kui põhikirja või ühingulepingu registrile esitamine on nõutav ka ühingu asukohamaal.

KAS uus § 82[4]. Seadusesse lisatakse eraldi paragrahv operatsiooniriski juhtimise nõuete sätestamiseks. Krediidiasutuse riskijuhtimise nõuete hulka kuulub mh DORA määruse rakendamine. Sealhulgas peavad krediidiasutus info- ja võrgusüsteemid olema loodud ja hallatud vastavalt DORA määruses sätestatule.

Kui KAS § 82 lõige 5 sätestab, et krediidiasutus peab kõigi oluliste äriprotsesside kohta välja töötama talitluspidevuse plaani majandustegevuse taastamise ja jätkuvuse tagamiseks, siis § 82[2] lõige 2 täpsustab, et selle üheks osaks on ka piisavate info- ja kommunikatsioonitehnoloogia talitluspidevuse põhimõtete ja plaanide ning reageerimis- ja taasteplaanide kehtestamine.

Tõhusaid talitluspidevuse ja taasteplaane on vaja selleks, et krediidiasustus saaks kohe ja kiiresti lahendada IKT intsidendid, eelkõige tulla toime küberrünnetega, piirates kahju ja seades prioriteediks tegevuse jätkamise ja taastemeetmed kooskõlas oma varunduspõhimõtetega. Sealjuures ei tohiks selline tegevuse jätkamine kuidagi seada ohtu võrgu- ja infosüsteemide terviklust ja turvalisust või andmete kättesaadavust, autentsust, terviklust ja konfidentsiaalsust.

DORA määruse kohaselt testib krediidiasutus kõiki funktsioone toetavate IKT-süsteemide IKT talitluspidevuse plaane ning IKT reageerimis- ja taasteplaane vähemalt kord aastas ja kriitilise tähtsusega või olulisi funktsioone toetavate IKT-süsteemide oluliste muudatuste korral. Sealjuures lisatakse testimisplaanidesse stsenaariumid, mis käsitlevad küberründeid ja esmase IKT-taristu ja varuvõimsuse vahelist ümberlülitust, varundamist ja varurajatisi.

Lõige 3. Kuna DORA määruse põhjenduspunktis nr 16 on selgitatud, et DORA määrus on NIS2 suhtes *lex specialis*, siis ei kohaldata krediidiasutuse suhtes neid KüTS sätteid, millega võetakse üle NIS2 teemad, mis on juba DORA määruses reguleeritud, näiteks sätted IKT riskijuhtimise, IKT intsidentide haldamise ja eelkõige tõsistest IKT intsidentidest teavitamise, samuti

[30] Äriseadustiku ja raamatupidamise seaduse muutmise seaduse (digilahendused äriühinguõiguses) eelnõu seletuskiri

digitaalse tegevuskerksuse testimise, teabevahetuse kokkulepete ja kolmandatest isikutest tulenevat IKT-riskide kohta.

Arvestades, et NIS2 nõudeid (KüTS muudatusi) hakatakse kohaldama DORA nõuetest kolm kuud varem, tasub õigusselguse huvides kaaluda, kas vastav välistus tuleks ette näha ka KüTSis.

KAS uus § 92[3]. DORA määruse artikli 19 lõike 1 kohaselt peab finantsasutus teavitama pädevat asutust (FI-d) tõsistest IKT-ga seotud intsidentidest. Lisaks annab määrus liikmesriigile võimaluse ette näha, et mõned või kõik finantssektori ettevõtjad esitavad pädevale asutusele või küberturbe intsidentide lahendamise üksustele, mis on määratud või loodud direktiivi (EL) 2022/2555 kohaselt, ka esialgse teate ja kõik raportid, kasutades DORA määruse artiklis 20 osutatud vorme (**lõiked 1 ja 2**). Lõikega 1 nähakse ette, et krediidiasutus teavitab lisaks FI-le ka RIA-t.

Intsidentide liigitamise kriteeriumid on ette nähtud DORA määruse art 18 lõikes 1, kuid täpsemad kriteeriumid tõsiste intsidentide määratlemiseks töötavad välja ESA-d koostöös EKP ja ENISA-ga.

Lisaks sätestab DORA määruse art 19 lõige 2, et finantsasutused võivad vabatahtlikult teatada asjaomasele pädevale asutusele olulistest küberohtudest, kui nad peavad ohtu finantssüsteemi, teenusekasutajate või klientide jaoks oluliseks, sealjuures võivad liikmesriigid otsustada, et need finantsasutused, kes teatavad vabatahtlikult esimese lõigu kohaselt, võivad kõnealuse teate edastada ka direktiivi (EL) 2022/2555 kohaselt määratud või loodud küberturbe intsidentide lahendamise üksustele.

KAS § 96 muutmine. Lõikesse 5 on lisatud viide digitaalse tegevuskerksuse testimise käigus tuvastatud riskile. Nimelt jälgib ja hindab FI, kas krediidiasutuse rakendatavad strateegiad, juhtimise korraldus, protseduurid, sealhulgas raamatupidamises rakendatavad protseduurid, aruandlussüsteemid ja sisekontroll on kooskõlas Euroopa Parlamendi ja nõukogu määruse (EL) nr 575/2013, krediidiasutuste seaduse ja muude õigusaktide nõuetega, selleks, et usaldusväärselt hinnata riske, sealhulgas süsteemset riski, digitaalse tegevuskerksuse testimise käigus ilmnenud riski ja stressitesti käigus ilmnenud riski. Nagu öeldud, uuendus on, et jälgida ja hinnata tuleb ka digitaalse testimise käigus tuvastatud riske.

Muudatuse aluseks on direktiivi 2013/36/EL art 97 lõike 1 muudatus. Lõikesse 1 on lisatud viide digitaalse tegevuskerksuse testimise käigus tuvastatud riskidele. Kuna sama artikli lõige 3 ütleb, et lõikes 1 osutatud läbivaatamisele ja hindamisele tuginedes otsustavad pädevad asutused, kas korrad, strateegiad, protsessid ja mehhanismid, mida finantsinstitutsioonid on rakendanud, ja nende omavahendid ning nende likviidsus tagavad riskide usaldusväärse juhtimise ja piisava katmise, käib see ka digitaalse tegevuskerksuse testimise käigus ilmnenud riskide kohta. Seega hindab FI § 96 lõike 5 kohaselt ka digitaalse tegevuskerksuse testimise käigus tuvastatud riskide puhul, kas likviidsus ja omavahendid on piisavad krediidiasutuse usaldusväärseks juhtimiseks ja riskide katmiseks.

KAS § 99 muutmine. Direktiivi 2013/36/EL artikkel 65 sätestab, kellelt pädeval asutusel on õigus nõuda teavet, mida ta vajab järelevalveliste ülesannete täitmiseks. Kehtivat nimekirja on täpsustatud viitega kolmandast isikust info-ja kommunikatsioonitehnoloogia teenuse osutajale. DORA määruse artikli 3 punkti 19 kohaselt on tegemist ettevõtjaga, kes osutab IKT-teenuseid. KAS § 99 lõike 1 punkt 4 küll sätestab juba, et FI-l on järelevalve teostamiseks õigus nõuda aruandeid, tasuta teavet, dokumente ning suulisi ja kirjalikke selgitusi järelevalve teostamisel tähtsust omavate asjaolude kohta mh kolmandalt isikult (põhjendatud vajaduse korral), kuid

selguse huvides on uues punktis 4^1 eraldi välja toodud, et selliseks isikuks on ka IKT teenuseosutaja.

KAS § 103 uus lõige 3^2. Paragrahv reguleerib ettekirjutuse tegemist ja muude meetmete rakendamist. Eelnõuga lisatakse paragrahvi uus lõige, milles sätestatakse, et FI-l on õigus rakendada DORA määruse artiklis 50 sätestatud õigusi ja meetmeid ning, et FI avalikustab vastavate meetmete alusel tehtud otsuse kohta teate oma veebilehel nagu on sätestatud artiklis 54.

Näiteks on FI-l õigus tutvuda kõigi dokumentidega või mis tahes vormis muude andmetega, mis võiksid olla FI ülesannete täitmiseks olulised, ja saada või teha nende dokumentide koopiaid, teha kohapealsed kontrolle või uurimisi ning nõuda määruse nõuete rikkumise korral parandus- ja ennetusmeetmete võtmist.

DORA määruse artikli 50 lõige 4 kohustab liikmesriike pädevatele asutustele andma õiguse kohaldada määruse nõuete rikkumise korral halduskaristusi või parandusmeetmeid. Sellisteks meetmeteks on:
- ettekirjutuse tegemine, et füüsiline või juriidiline isik lõpetaks rikkuva tegevuse ja hoiduks selle tegevuse kordamisest;
- sellise tegevuse või tava peatamise nõudmine, mis on vastuolus määruse sätetega;
- mis tahes liiki meetmete võtmine, sealhulgas rahaliste meetmete, tagamaks, et finantsasutused jätkavad õigusnormide järgimist;
- liikmesriigi õigusega lubatud ulatuses sideoperaatorite valduses olete andmeliiklusandmete nõudmine, kui on piisav alus kahtlustada määruse nõuete rikkumist ja kui sellised andmed võivad olla olulised määruse rikkumiste uurimisel, ning
- avalike teadaannete väljastamine, mis sisaldavad füüsilise või juriidilise isiku identiteeti ja rikkumise laadi.

Et võetud meetmetel oleks hoiatav mõju laiemale avalikkusele, näeb määrus ette rikkumist puudutavate otsuste ja rakendatud meetmete avalikustamise. DORA määruse artikli 54 lõike 1 kohaselt avaldavad pädevad asutused oma ametlikel veebisaitidel põhjendamatu viivituseta kõik halduskaristuse määramise otsused, mida ei ole edasi kaevatud pärast seda, kui karistuse saanud isikut on otsusest teavitatud. Avaldada tuleb teave rikkumise liigi ja laadi kohta, vastutavad isikud ning määratud karistused. Erandiks on olukorrad, kus juriidilise isiku nime või füüsilise isiku nime ja isikuandmete avaldamine oleksid ebaproportsionaalsed või nende andmete avaldamine ohustaks finantsturgude stabiilsust või pooleli olevat uurimist (eelkõige mõeldud järelevalve- ja väärteomenetlust, kuid võib hõlmata ka kriminaalmenetlust tegevusloata tegutsemise puhul) või põhjustaks asjaomasele isikule ebaproportsionaalselt suurt kahju. Sellisel puhul võib avaldamise edasi lükata, jätta isikuid puudutav teave avaldamata või loobuda sellise kaasuse kohta teabe avaldamisest üldse.

KAS §-de 134^{23}–134^{25} kehtetuks tunnistamine. Kuna eelnõuga lisandub vastutuse peatükki uus paragrahv uue koosseisuga, tunnistatakse kehtetuks paragrahvid, mis oma sisult peaksid olema vastutuse peatüki kolm kõige viimast paragrahvi – paragrahv, mis selgitab, kuidas määrata juriidilise isiku ja konsolideerimisgrupi käivet trahvi suuruse arvutamisel, paragrahv väärtegude aegumise kohta ning paragrahv väärtegude menetleja kohta. Paragrahvid sätestatakse uuesti §-des 140^1–140^3.

KAS uus § 134^{26}. Seadust täiendatakse uue karistusnormiga, mida FI saab kohaldada DORA määruses sätestatud nõuete rikkumise korral. Nimelt on DORA määruse artikli 50 lõikes 3 sätestatud, et liikmesriigid kehtestavad õigusnormid, milles sätestatakse asjakohased halduskaristused ja parandusmeetmed määruse rikkumise puhuks, ning tagavad nende

tulemusliku rakendamise. Sama artikli lõike 4 punktis c on sätestatud, et liikmesriigid annavad pädevatele asutustele õiguse võtta mis tahes liiki meetmeid, sealhulgas rahalisi meetmeid, tagamaks, et finantssektori ettevõtjad jätkavad õigusnormide järgimist. Eelnõuga nähakse ette, et füüsilise isiku korral on võimalik karistada rahatrahviga kuni 5 000 000 eurot või kuni kahekordse väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas ning juriidilise isiku korral karistatakse rahatrahviga kuni 5 000 000 eurot või kuni kahekordse väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas või kuni kümme protsenti juriidilise isiku või tema konsolideerimisgrupi konsolideeritud käibest.

Uue paragrahvi lõike 1 sõnastuses on viidatud järgmistele DORA määruse nõuete rikkumistele:
- art 5–14: IKT- riski juhtimine;
- art 16–18, art 19 lõiked 1–5: IKT intsidentide haldamine ja liigitamine ning nendest teavitamine;
- art 24, 25, art 27 lõiked 1–8: digitaalse tegevuskerksuse testimine;
- art 28 lõiked 1–8, art 29, art 30 lõiked 1–4: kolmandast isikust tuleneva IKT-riski juhtimine;
- art 42 lg 3: kolmanda isikuga seotud riskide arvesse võtmine.

KAS uued paragrahvi. 2002. aastal[31] tunnistati kehtetuks KAS §-d 135–140, mistõttu on kehtetuks tunnistatud §-de 134^{23}–134^{25} uuesti sõnastamisel kasutatud numeratsiooni 140^{1}–140^{3}, vältimaks, et iga kord peab samad paragrahvid uuesti kehtetuks tunnistama ja uuesti kehtestama, kui on soov lisada vastutuse peatükki uued karistuse paragrahvid.

Seaduse normitehniline märkus. Muudatusega lisatakse viide DORA direktiivile.

3.8. Eelnõu § 8. Makseasutuste ja e-raha asutuste seaduse muutmine

Direktiivis (EL) 2015/2366 on sätestatud erinormid IKT turvalisuskontrollide ja riskimaanduselementide kohta seoses makseteenuste osutamiseks tegevusloa saamisega. Loa andmise norme on direktiivis muudetud, et viia need kooskõlla DORA määrusega. Lisaks võimaldatakse makseasutustel kasutada ühtset, täielikult ühtlustatud intsidentidest teatamise mehhanismi seoses kõigi operatsiooni- ja turvaintsidentidega, olenemata sellest, kas need on maksetega seotud või mitte.

MERAS § 3 muutmine (ei ole seotud DORA direktiiviga, seaduses parandatakse EL määruse nimetus õigeks)**.** Euroopa Parlamendi ja Nõukogu määrusega (EL) 2019/2033, 27. november 2019, mis käsitleb investeerimisühingute suhtes kohaldatavaid usaldatavusnõudeid ning millega muudetakse määrusi (EL) nr 1093/2010, (EL) nr 575/2013, (EL) nr 600/2014 ja (EL) nr 806/2014, muudeti Euroopa Parlamendi ja nõukogu määruse (EL) nr 575/2013 pealkirja, mistõttu viiakse MERAS-es olev viide määrusele kooskõlla selle õige nimetusega.

MERAS § 4 lõike 1 punkti 9 muutmine. Paragrahvis 4 on reguleeritud, milliseid teenuseid ei peeta makseteenusteks. Muudatus on terminoloogiline ning infotehnoloogiaalase teenuse asemel kasutatakse terminit info- ja kommunikatsioonitehnoloogiateenus. Muudatuse aluseks on DORA direktiiviga direktiivi 2015/2366 artikli 3 punkti j muutmine.

MERAS § 7 lõike 1 muutmine (ei ole seotud DORA direktiiviga)**.** Muudatusega kehtestatakse piirang, mille kohaselt võib e-raha asutus tegutseda üksnes aktsiaseltsina, kui ta osutab mh makseteenuseid. Kehtiva seaduse kohaselt saab e-raha asutus osutada teatud makseteenuseid osaühinguna, kuigi makseasutus peab samade teenuste osutamiseks olema aktsiaselts.

[31] https://www.riigiteataja.ee/akt/212735

MERAS § 15 lõike 1 punkti 9 muutmine. Makseteenuste osutamise tegevusloa taotlemisel tuleb FI-le muu hulgas esitada info- ja kommunikatsiooniteenuste kasutamise kord. IKT-teenus on defineeritud DORA määruse artikli 3 punktis 21. Tegemist on digi- ja andmeteenusega, mida osutatakse pidevalt IKT-süsteemide kaudu ühele või mitmele sise- või väliskasutajale, sealhulgas riistvara teenusena ja riistvarateenused, mis hõlmab tehnilise toe pakkumist riistvara pakkuja tarkvara- või püsivarauuenduste kaudu (va tavapärased analoogtelefoniteenused).

MERAS § 15 lõike 1^1 punktis 2 on täpsustatud, mida peab sisaldama turvapoliitika kirjeldus, mis tuleb tegevusloa taotlemisel FI-le esitada. Muudatusega täpsustatakse, et turvapoliitika kirjeldus peaks sisaldama mh selgitust, kuidas tagatakse digitaalsele tegevuskerksuse kõrge tase, järgides sealjuures DORA määruse IKT riskijuhtimise nõudeid.

MERAS § 32 lõike 2 punkti 6 muutmine ja uus punkt 6^1 (ei ole seotud DORA direktiiviga, kuid on tehniline muudatus, et vältida seaduses olevat tühja viidet). Kuna ÄS § 386 lõike 2 punkt 4 on tunnistatud kehtetuks, korrigeeritakse MERAS sõnastust ja kustutatakse viide kehtetule ÄS punktile 4. ÄS-ist välja jäetud punkt sõnastatakse MERAS-es. Seega peab kolmanda riigi makseasutus või e-raha asutus Eestis filiaali asutamise loa taotlemisel esitama FI-le äriühingu põhikirja või ühingulepingu asukohamaa seaduste kohaselt tõestatud ärakirja, kui põhikirja või ühingulepingu registrile esitamine on nõutav ka ühingu asukohamaal.

MERAS § 50 lõike 3 punkti 6 muutmine. Terminoloogiline muudatus, kus termin infotehnoloogiaalase asemel kasutatakse terminit info- ja kommunikatsioonitehnoloogia.

MERAS § 50 lõike 3 punkti 9 muutmine. Makseasutuses ja e-raha asutuses peab sise-eeskirjadega kehtestama intsidentidest teatamise korra. Korra kehtestamisel tuleks arvesse võtta DORA määruse kolmandas peatükis sätestatud IKT intsidentide haldamise ja liigitamise ning intsidentidest teavitamise nõudeid. DORA määruse kolmandas peatükis sätestatud nõudeid kohaldatakse ka tegevust või turvalisust mõjutavate maksetega seotud intsidentide ning tegevust või turvalisust mõjutavate maksetega seotud tõsiste intsidentide suhtes.

MERAS § 50 lõike 3 punkti 11 muutmine. Kehtivasse sõnastusse on lisatud viide DORA määrusele, milles sätestatut tuleb arvesse võtta info- ja kommunikatsioonitehnoloogia talitluspidevuse põhimõtete ja plaanide ning info- ja kommunikatsioonitehnoloogia reageerimis- ja taasteplaanide koostamisel ja kehtestamisel, testimisel ja läbivaatamisel.

Tõhusaid talitluspidevuse ja taasteplaane on vaja selleks, et makseasutus saaks kohe ja kiiresti lahendada IKT intsidendid, eelkõige tulla toime küberrünnetega, piirates kahju ja seades prioriteediks tegevuse jätkamise ja taastemeetmed kooskõlas oma varunduspõhimõtetega. Sealjuures ei tohiks selline tegevuse jätkamine kuidagi seada ohtu võrgu- ja infosüsteemide terviklust ja turvalisust või andmete kättesaadavust, autentsust, terviklust ja konfidentsiaalsust.

Makseasutus testib kõiki funktsioone toetavate IKT-süsteemide IKT talitluspidevuse plaane ning IKT reageerimis- ja taasteplaane vähemalt kord aastas ja kriitilise tähtsusega või olulisi funktsioone toetavate IKT-süsteemide oluliste muudatuste korral. Sealjuures lisatakse testimisplaanidesse stsenaariumid, mis käsitlevad küberründeid ja esmase IKT-taristu ja varuvõimsuse vahelist ümberlülitust, varundamist ja varurajatisi.

MERAS § 52 muutmine (ei ole seotud DORA direktiiviga)**.** Kui kehtiva õiguse kohaselt on makseasutuste ja e-raha asutuste ümberkujundamine keelatud, siis eelnõuga lubatakse riigisisest ümberkujundamist osaühingust aktsiaseltsiks. Makseasutus või e-raha asutus saab seda siiski teha vaid FI loal (**lõige 1**), mis on täiendav tingimus võrreldes äriseadustikus sätestatuga.

Olukorras, kus piiratud makseteenuste osutamisega alustanud ning osaühinguna registreeritud makseasutus soovib osutada makseteenuseid, mida võib MERAS § 5 lõike 1 kohaselt osutada aktsiaseltsina asutatud makseasutus, siis tuleks osaühinguna registreeritud asutus likvideerida ja asutada uus makseasutus või asutada uus makseasutus, millega olemasolev ühendada. Tulenevalt eeltoodust lubatakse osaühingust asutust ümber kujundada aktsiaseltsiks.

Lõikes 1[1]. Osaühinguna asutatud asutuse ümber kujundamiseks aktsiaseltsiks peab ettevõtja järgima muu hulgas äriseadustikus sätestatud nõudeid ja kohandama ettevõtte tegevuse vastavaks.

Lõikes 1[2] on loetelu teabest, mis tuleb FI-le loa saamiseks esitada. Kuna lubatud on asutust vaid osaühingust aktsiaseltsiks ümber kujundada, siis tuleb esitada selle osaühingu osanike koosoleku otsus põhikirja muutmise kohta ja põhikirja muudetud tekst, osanike koosoleku protokoll ja ümberkujundamisaruanne. Täpsemad nõuded sätestavad eelnimetatud aruandele ÄS § 479 lõiked 1–2.

Lõige 1[3] sätestab finantsjärelevalve asutusele ajaraamistiku, mille jooksul peab FI tegema motiveeritud otsuse ümberkujundamiseks nõusoleku andmise või sellest keeldumise kohta. Nimetatud lõike kohaselt teeb FI ümberkujundamise otsuse kohta otsuse nõusoleku andmise või sellest keeldumise kohta üldjuhul ühe kuu jooksul alates nõuetekohaste dokumentide ja andmete saamisest. Maksimaalselt võib nimetatud otsuse tegemine aega võtta kolm kuud ümberkujundamistaotluse esitamisest.

Lõige 1[4] kehtestab finantsjärelevalvele õiguse keelduda ümberkujundamise loa andmisest. Kuivõrd loa andmisest keeldumisega kaasneb tugev isiku õiguste riive, siis on konkreetsemad ümberkujundamise keeldumise alused äärmiselt olulised. Lõike kohaselt võib FI keelduda ümberkujundamise loa andmisest, kui ümberkujundamise luba taotleva makseasutuse või e-raha asutuse finantsseisund ei vasta MERAS-es sätestatud nõuetele (punkt 1) või ümberkujundamisega seotud dokumentatsioon ei vasta MERAS-es või muudes õigusaktides sätestatud nõuetele (punkt 2). Kui ümberkujundamine võib muul põhjusel kahjustada klientide huve (punkt 3), on FI-l samuti õigus keelduda ümberkujundamise loa andmisest. Samuti on oluline, et finantsjärelevalve õigus keelduda ei oleks piiratud üksnes eelnimetatud olukordadega, vaid kui esineb muu oluline alus ümberkujundamise mittelubamiseks, siis punkt 4 annab selle aluse.

Lõige 1[5] sätestab, et äriregistrile esitatavale avaldusele lisatakse FI luba teenuseosutaja ümberkujundamiseks, millest tulenevalt on vajalik saada FI luba enne ümberkujundamise lõpuleviimist äriregistri kandega.

Lõike 1[6] kohaselt avalikustab FI ümberkujundamisloa andmise otsuse hiljemalt otsuse tegemisele järgneval tööpäeval oma veebilehel.

Lõige 1[7]. Kuigi eelnõuga muudetakse makseasutuse ja e-raha asutuste ümberkujundamist paindlikumaks, siis piiriülene ümberkujundamine ei ole jätkuvalt lubatud, kuna piiriülese ümberkujundamisega ei ole tagatud piisav klientide huvide kaitse.

MERAS § 62 lõike 2 ja § 84 lõike 2 punkti 4 muutmine. Terminoloogiline täpsustus, kus infotehnoloogia asendatakse terminiga info- ja kommunikatsioonitehnoloogia.

MERAS § 63[5] uus lõige 3. Makseasutus ja e-raha asutus on kohustatud järgima DORA määruses sätestatud digitaalse tegevuskerksuse nõudeid. DORA kohaldamisulatusse kuuluvad

kõik makseasutused, sealhulgas sellised makseasutused, mille suhtes kohaldatakse direktiivi (EL) 2015/2366 artikli 32 lõike 1 kohast erandit (MERAS § 11 lg 1 ja 2) ja kontoteabeteenuse osutajad (makseasutused, mis osutavad MERAS § 3 lõike 1 punktis 8 osutatud teenust) ning kõik e-raha asutused, sealhulgas e-raha asutused, mille suhtes kohaldatakse direktiivi 2009/110/EÜ artikli 9 lõike 1 kohast erandit (MERAS § 12 lõikes 1 nimetatud e-raha asutused).

DORA määruse artikli 16 kohaselt kohaldatakse erandi alla kuuluvatele makseasutustele ja e-raha asutustele lihtsustatud IKT riskijuhtimise raamitiku nõudeid.

MERAS § 63^6 pealkirja muutmine. Kuna paragrahvi lisandub ka küberohtudest teavitamine, viiakse paragrahvi pealkiri kooskõlla selle sisuga.

MERAS § 63^6 täiendamine uute lõigetega 5–8.

Lõige 5. Kuna makseasutustele ja e-raha asutustele hakkab kohalduma DORA määruses sätestatud intsidentidest teatamise kord, on §-i 63^6 lisatud täpsustus, et DORA määruse kohaldamisalasse kuuluvad makseasutused ja e-raha asutused, sealhulgas erandi alla kuuluvad ja kontoteabe osutajad, lähtuvad operatsiooni- või turvaintsidendist teavitamisel (nii FI kui ka klientide teavitamisel) DORA määruses sätestatust (DORA määrus kasutab terminit „tegevust või turvalisust mõjutav maksetega seotud intsident“). Lõigetes 1 ja 2 sätestatu jääb kohalduma ülejäänutele makseteenuse pakkujatele. Nimelt näeb DORA määruse artikkel 23 ette, et DORA määruse peatükis 3 sätestatud nõudeid kohaldatakse ka tegevust või turvalisust mõjutavate maksetega seotud intsidentide ning tegevust või turvalisust mõjutavate maksetega seotud tõsiste intsidentide suhtes, kui need puudutavad krediidiasutusi, makseasutusi, kontoteabe teenuse pakkujaid ning e-raha asutusi.

Intsident	**IKT-intsident**	**Tegevust või turvalisust mõjutav maksetega seotud intsident**
Finantssektori ettevõtja poolt planeerimata üksiksündmus või omavahel seotud sündmuste jada, mis:	- seab ohtu võrgu- ja infosüsteemide turvalisuse; - avaldab negatiivset mõju andmete kättesaadavusele, autentsusele, terviklusele või konfidentsiaalsusele või finantssektori ettevõtja osutatavatele teenustele.	- avaldab negatiivset mõju maksete andmete kättesaadavusele, autentsusele, terviklusele või konfidentsiaalsusele või finantssektori ettevõtja osutatud maksetega seotud teenustele, olenemata sellest, kas need sündmused on IKTga seotud.
	Tõsine IKT intsident	**Tõsine tegevust või turvalisust mõjutav maksetega seotud intsident**
	- millel on suur negatiivne mõju võrgu- ja infosüsteemidele, mis toetavad finantssektori ettevõtja kriitilise tähtsusega või olulisi funktsioone.	- avaldab suurt negatiivset mõju osutatud maksetega seotud teenustele.

Makseasutused ja e-raha asutused peavad DORA-s sätestatud eeskirjade alusel teavitama FI-d nii tõsistest IKT-ga seotud intsidentidest kui ka osutatava makseteenusega seotud olulistest operatsiooni- või turvaintsidentidest.

Lõike 6 kohaselt tuleb IKT-ga seotud tõsistest intsidentidest teavitada lisaks FI-le ka RIA-t. Operatsiooni- või turvaintsidentidest teavitatakse üksnes FI-d. Sealjuures tuleb kirjeldatud intsidentide puhul kasutada DORA määruse alusel kehtestatud teavitusvorme ja lähtuda teavitamisel DORA alusel kehtestatud tähtaegadest.

Lisaks sätestab DORA määruse artikli 19 lõige 2, et finantsasutused võivad vabatahtlikult teatada asjaomasele pädevale asutusele olulistest küberohtudest, kui nad peavad ohtu finantssüsteemi, teenusekasutajate või klientide jaoks oluliseks, sealjuures võivad liikmesriigid otsustada, et need finantsasutused, kes teatavad vabatahtlikult esimese lõigu kohaselt, võivad kõnealuse teate edastada ka direktiivi (EL) 2022/2555 kohaselt määratud või loodud küberturbe intsidentide lahendamise üksustele (**lõige 8**).

Kuivõrd FIS § 46^2 lõikes 8 on sätestatud, et Inspektsioon teavitab pärast MERAS § 63^6 lõikes 1 nimetatud teate saamist viivitamata Euroopa Pangandusjärelevalve Asutust ja Euroopa Keskpanka olulisest operatsiooni- või turvaintsidendist, siis see kohaldub selliste teadete suhtes, mis jäävad MERAS § 63^6 lõike 1 kohase teavitamise alla. DORA määruse kohaselt saadud teated edastab FI EBA-le ja Euroopa Keskpangale DORA määruse artikli 19 lõike 6 kohaselt.

MERAS § 91 muutmine. Paragrahvi pealkiri viiakse kooskõlla selle sisuga, kuivõrd eelnõuga lisatakse paragrahvi uus lõige, milles sätestatakse, et FI-l on õigus rakendada DORA määruse artiklis 50 sätestatud õigusi ja meetmeid ning FI avalikustab vastavate meetmete alusel tehtud otsuse kohta teate oma veebilehel, nagu on sätestatud määruse artiklis 54.

Näiteks on FI-l õigus tutvuda kõigi dokumentidega või mis tahes vormis muude andmetega, mis võiksid olla FI ülesannete täitmiseks olulised, ja saada või teha nende dokumentide koopiaid, teha kohapealsed kontrolle või uurimisi ning nõuda määruse nõuete rikkumise korral parandus- ja ennetusmeetmete võtmist.

DORA määruse artikli 50 lõige 4 kohustab liikmesriike pädevatele asutustele andma õiguse kohaldada määruse nõuete rikkumise korral halduskaristusi või parandusmeetmeid. Sellisteks meetmeteks on:

- ettekirjutuse tegemine, et füüsiline või juriidiline isik lõpetaks rikkuva tegevuse ja hoiduks selle tegevuse kordamisest;
- sellise tegevuse või tava peatamise nõudmine, mis on vastuolus määruse sätetega;
- mis tahes liiki meetmete võtmine, sealhulgas rahaliste meetmete, tagamaks, et finantsasutused jätkavad õigusnormide järgimist;
- liikmesriigi õigusega lubatud ulatuses sideoperaatorite valduses olete andmeliiklusandmete nõudmine, kui on piisav alus kahtlustada määruse nõuete rikkumist ja kui sellised andmed võivad olla olulised määruse rikkumiste uurimisel, ning
- avalike teadaannete väljastamine, mis sisaldavad füüsilise või juriidilise isiku identiteeti ja rikkumise laadi.

Et võetud meetmetel oleks hoiatav mõju laiemale avalikkusele, näeb määrus ette rikkumist puudutavate otsuste ja rakendatud meetmete avalikustamise. DORA määruse artikli 54 lõike 1 kohaselt avaldavad pädevad asutused oma ametlikel veebisaitidel põhjendamatu viivituseta kõik halduskaristuse määramise otsused, mida ei ole edasi kaevatud pärast seda, kui karistuse saanud isikut on otsusest teavitatud. Avaldada tuleb teave rikkumise liigi ja laadi kohta,

vastutavad isikud ning määratud karistused. Erandiks on olukorrad, kus juriidilise isiku nime või füüsilise isiku nime ja isikuandmete avaldamine oleksid ebaproportsionaalsed või nende andmete avaldamine ohustaks finantsturgude stabiilsust või pooleli olevat uurimist (eelkõige mõeldud järelevalve- ja väärteomenetlust, kuid võib hõlmata ka kriminaalmenetlust tegevusloata tegutsemise puhul) või põhjustaks asjaomasele isikule ebaproportsionaalselt suurt kahju. Sellisel puhul võib avaldamise edasi lükata, jätta isikuid puudutav teave avaldamata või loobuda sellise kaasuse kohta teabe avaldamisest üldse.

MERAS uus § 109[1]. Seadust täiendatakse uue karistusnormiga, mida FI saab kohaldada DORA määruses sätestatud nõuete rikkumise korral. Nimelt on DORA määruse artikli 50 lõikes 3 sätestatud, et liikmesriigid kehtestavad õigusnormid, milles sätestatakse asjakohased halduskaristused ja parandusmeetmed määruse rikkumise puhuks, ning tagavad nende tulemusliku rakendamise. Sama artikli lõike 4 punktis c on sätestatud, et liikmesriigid annavad pädevatele asutustele õiguse võtta mis tahes liiki meetmeid, sealhulgas rahalisi meetmeid, tagamaks, et finantssektori ettevõtjad jätkavad õigusnormide järgimist. Eelnõuga nähakse ette, et füüsilise isiku korral on võimalik karistada rahatrahviga kuni 5 000 000 eurot või kuni kahekordse väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas ning juriidilise isiku korral karistatakse rahatrahviga kuni 5 000 000 eurot või kuni kahekordse väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas või kuni kümme protsenti juriidilise isiku või tema konsolideerimisgrupi konsolideeritud käibest

Uue paragrahvi lõike 1 sõnastuses on viidatud järgmistele DORA määruse nõuete rikkumistele:
- art 5–14: IKT- riski juhtimine;
- art 16–18, art 19 lõiked 1–5: IKT intsidentide haldamine ja liigitamine ning nendest teavitamine;
- art 24, 25, art 27 lõiked 1–8: digitaalse tegevuskerksuse testimine;
- art 28 lõiked 1–8, art 29, art 30 lõiked 1–4: kolmandast isikust tuleneva IKT-riski juhtimine;
- art 42 lg 3: kolmanda isikuga seotud riskide arvesse võtmine.

Seaduse normitehniline märkus. Muudatusega lisatakse viide DORA direktiivile.

3.9. Eelnõu § 9. Väärtpaberite registri pidamise seaduse muutmine

EVKS § 7[1] lõike 5 muutmine ja lõike 7 kustutamine. 2022. aasta 16. augustil jõustusid KüTS muudatused, millega ühtlasi tunnistati kehtetuks avaliku teabe seaduse (AvTS) § 43[9] lõike 1 punktis 4 sätestatud Vabariigi Valitsuse volitusnorm infosüsteemide turvameetmete süsteemi kehtestamiseks, millele EVKS § 7[1] kehtivas lõikes 7 on viidatud. Volitusnormi kustutamist on selgitatud järgmiselt: „Kuna eelnõuga luuakse KüTS-is võimalus kehtestada E-ITS[32], siis tuleb ISKE[33] määruse volitusnorm tunnistada kehtetuks. /…/ E-ITS-i määruse volitusnormi paiknemine KüTS-is ja selle rakendusaktides on avaliku teabe töötlemist ja küberturvalisust reguleerivaid õigusakte, nende omavahelisi seoseid ning struktuuri arvesse võttes mõistlik“.

Seega tunnistatakse lõige 7 kehtetuks, kuna viitab kehtetule AvTS volitusnormile. Registripidajale hakkavad kohalduma DORA määruse turvastandardid.

Kuna lõikes 5 on viide lõikele 7, mis tunnistatakse kehtetuks, tuleb muuta ka lõike 5 sõnastust ja sealt välja jätta viide lõikele 7.

---

[32] Eesti infoturbestandard, https://www.riigiteataja.ee/aktilisa/1211/2202/2034/MKM_m101_lisa.pdf#

[33] infosüsteemide kolmeastmelise etalonturbe süsteem

EVKS täiendamine uue §-ga 30[2] nähakse ette uus paragrahv digitaalse tegevuskerksuse nõuete rakendamiseks.

Lõige 1. DORA määruse artikli 2 lõike 1 punkti g kohaselt kuuluvad väärtpaberite keskdepositooriumid samuti DORA kohaldamisalasse. Kuigi tegemist on otsekohalduva määrusega, on selguse huvides lõikes 1 viide DORA määruse nõuete rakendamisele.

Lõige 2. KüTS § 3 lõike 4 punkti 1 kohaselt kohaldatakse KüTS-is teenuse osutaja kohta sätestatut ka andmekogu vastutavale töötlejale ja volitatud töötlejale. Muudatust on eelnevalt selgitatud järgmiselt: „Andmekogude vastutavate ja volitatud töötleja hõlmamine avaliku sektori loetelu alla on vajalik ka põhjusel, et eelnõu asendab AvTS-i alusel kehtestatud ISKE KüTS-i alusel kehtestava E-ITS-iga ning selleks, et tagada andmekogude küberturvalisus, tuleb seega ka täpsustada KüTS-i kohaldamisala.“ Andmekogu on andmekogu AvTS § 43[1] lõike 1 tähenduses (andmekogu on riigi, kohaliku omavalitsuse või muu avalik-õigusliku isiku või avalikke ülesandeid täitva eraõigusliku isiku infosüsteemis töödeldavate korrastatud andmete kogum, mis asutatakse ja mida kasutatakse seaduses, selle alusel antud õigusaktis või rahvusvahelises lepingus sätestatud ülesannete täitmiseks).

EVKS § 1[2] lõike 2 kohaselt on Eesti väärtpaberite register riigi infosüsteemi kuuluv andmekogu aktsiate, võlakohustuste ja teiste EVKS § 2 lõigetes 1 ja 2 nimetatud väärtpaberite ning nende väärtpaberitega tehtavate toimingute registreerimiseks. Registripidaja on keskdepositoorium, kellele on antud õigus registrit pidada.

Kuna registripidaja peab lõike 1 kohaselt juba rakendama DORA määruses sätestatud IKT-riskide juhtimise ja intsidentidest teavitamise nõudeid ja vältimaks nõuete dubleerimist, nähakse lõikega 2 ette, et registripidajale ei kohaldata KüTS-i neid sätteid, mis on juba kaetud DORA määrusega. NIS 2 direktiivi põhjenduspunkti 28 kohaselt tuleks NIS2 direktiivi sätete asemel kohaldada DORA määruse sätteid, mis käsitlevad IKT riskijuhtimist, IKT intsidentide haldamist ja eelkõige tõsistest IKT intsidentidest teavitamist, samuti digitaalse tegevuskerksuse testimist, teabevahetuse kokkuleppeid ja kolmandatest isikutest tulenevat IKT-riski. Seetõttu ei tohiks liikmesriigid NIS2 direktiivi sätteid, mis käsitlevad küberturvalisuse riskijuhtimist ja teatamiskohustust, järelevalvet ja täitmise tagamist, DORA määruse kohaldamisalasse jäävate finantssektori ettevõtjate suhtes kohaldada.

Lõiked 3 ja 4. DORA määruse artikli 19 lõike 1 kohaselt peab finantsasutus teavitama pädevat asutust tõsistest IKT-ga seotud intsidentidest. Lisaks annab määrus liikmesriigile võimaluse ette näha, et mõned või kõik finantssektori ettevõtjad esitavad pädevale asutusele või küberturbe intsidentide lahendamise üksustele, mis on määratud või loodud direktiivi (EL) 2022/2555 kohaselt, ka esialgse teate ja kõik raportid, kasutades DORA määruse artiklis 20 osutatud vorme. Lõikega 3 nähakse ette, et registripidaja teavitab lisaks FI-le ka RIA-t.

Intsidentide liigitamise kriteeriumid on ette nähtud DORA määruse artikli 18 lõikes 1, kuid täpsemad kriteeriumid tõsiste intsidentide määratlemiseks töötavad välja ESA-d koostöös EKP ja ENISA-ga.

Lõige 5. Lisaks sätestab DORA määruse artikli 19 lõige 2, et finantsasutused võivad vabatahtlikult teatada asjaomasele pädevale asutusele olulistest küberohtudest, kui nad peavad ohtu finantssüsteemi, teenusekasutajate või klientide jaoks oluliseks, sealjuures võivad liikmesriigid otsustada, et need finantsasutused, kes teatavad vabatahtlikult esimese lõigu kohaselt, võivad kõnealuse teate edastada ka direktiivi (EL) 2022/2555 kohaselt määratud või loodud küberturbe intsidentide lahendamise üksustele.

Lõike 6 eesmärk on juhtida tähelepanu spetsiifilisele sättele, mille kohaselt peab DORA määrusest tulenevalt olema keskdepositooriumil vähemalt üks varutöötluskoht, millel on ärivajaduste rahuldamiseks piisavad ressursid, võimed, funktsioonid ja personalikorraldus. DORA määruse artikli 12 lõike 5 kohaselt peab varutöötluskoht asuma peamisest töötluskohast geograafiliselt eemal, et tagada nende erinev riskiprofiil ja vältida, et varutöötluskohta kahjustab peamisele töötluskohale mõju avaldanud sündmus. Lisaks peab see varutöötluskoht suutma tagada peamise töötluskohaga kriitilise tähtsusega või oluliste funktsioonide järjepidevuse või sellise teenuse taseme, mida on vaja, et saaks täita oma kriitilise tähtsusega funktsioone vastavalt taaste-eesmärkidele. See koht peaks olema registripidaja töötajatele kohe ligipääsetav.

Lõige 7. DORA määruse artikli 2 lõike 1 punkti g kohaselt kuuluvad DORA määruse kohaldamisalasse väärtpaberite keskdepositooriumid, kes on defineeritud määruse artikli 3 punktis 42. Tegemist on määruse (EL) nr 909/2014 (CSDR) artikli 2 lõike 1 punktis 1 määratletud väärtpaberite keskdepositooriumidega. Eesti väärtpaberite keskregistri seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse[34] seletuskirjas on selgitatud, et pensioniosakud ei kuulu CSDR-määruse reguleerimisalasse. Seega ei kuulu pensioniregistri pidaja ka DORA määruse kohaldamisalasse. Kuigi EVKS § 1^3 lõike 3 kohaselt kohaldatakse pensioniregistri pidajale ja selle pidamisele seaduses registripidaja ja registri kohta sätestatut, kui käesolevast seadusest ei tulene teisiti, siis lõike 7 eesmärk on õigusselguse mõttes täpsustata, et pensioniregistri pidajale kohaldatakse ka DORA määruse nõudeid (vt selgitust IFS § 345 juures seoses pensionifondi valitsejatele DORA määruse kohaldamisega).

EVKS § 38 uue lõike 1^3 kohaselt teostab FI järelevalvet DORA määruses sätestatud nõuete täitmise üle.

EVKS § 39 lõike 1 teise lausesse lisatakse viide DORA määrusele.

EVKS § 39 uus lõige 4^1 . FI peab avalikustama DORA määruse artikli 50 kohaselt võetud meetmete alusel tehtud otsuse kohta teate oma veebilehel nagu on sätestatud artiklis 54.

Näiteks on FI-l õigus tutvuda kõigi dokumentidega või mis tahes vormis muude andmetega, mis võiksid olla FI ülesannete täitmiseks olulised, ja saada või teha nende dokumentide koopiaid, teha kohapealsed kontrolle või uurimisi ning nõuda määruse nõuete rikkumise korral parandus- ja ennetusmeetmete võtmist.

DORA määruse artikli 50 lõige 4 kohustab liikmesriike pädevatele asutustele andma õiguse kohaldada määruse nõuete rikkumise korral halduskaristusi või parandusmeetmeid. Sellisteks meetmeteks on:

- ettekirjutuse tegemine, et füüsiline või juriidiline isik lõpetaks rikkuva tegevuse ja hoiduks selle tegevuse kordamisest;
- sellise tegevuse või tava peatamise nõudmine, mis on vastuolus määruse sätetega;
- mis tahes liiki meetmete võtmine, sealhulgas rahaliste meetmete, tagamaks, et finantsasutused jätkavad õigusnormide järgimist;
- liikmesriigi õigusega lubatud ulatuses sideoperaatorite valduses olete andmeliiklusandmete nõudmine, kui on piisav alus kahtlustada määruse nõuete rikkumist ja kui sellised andmed võivad olla olulised määruse rikkumiste uurimisel, ning
- avalike teadaannete väljastamine, mis sisaldavad füüsilise või juriidilise isiku identiteeti ja rikkumise laadi.

---

[34] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/cec5e4d6-98a5-4016-965a-c151c9e94354/eesti-vaartpaberite-keskregistri-seaduse-muutmise-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus

Et võetud meetmetel oleks hoiatav mõju laiemale avalikkusele, näeb määrus ette rikkumist puudutavate otsuste ja rakendatud meetmete avalikustamise. DORA määruse artikli 54 lõike 1 kohaselt avaldavad pädevad asutused oma ametlikel veebisaitidel põhjendamatu viivituseta kõik halduskaristuse määramise otsused, mida ei ole edasi kaevatud pärast seda, kui karistuse saanud isikut on otsusest teavitatud. Avaldada tuleb teave rikkumise liigi ja laadi kohta, vastutavad isikud ning määratud karistused. Erandiks on olukorrad, kus juriidilise isiku nime või füüsilise isiku nime ja isikuandmete avaldamine oleksid ebaproportsionaalsed või nende andmete avaldamine ohustaks finantsturgude stabiilsust või pooleli olevat uurimist (eelkõige mõeldud järelevalve- ja väärteomenetlust, kuid võib hõlmata ka kriminaalmenetlust tegevusloata tegutsemise puhul) või põhjustaks asjaomasele isikule ebaproportsionaalselt suurt kahju. Sellisel puhul võib avaldamise edasi lükata, jätta isikuid puudutav teave avaldamata või loobuda sellise kaasuse kohta teabe avaldamisest üldse.

EVKS §-de 46^{8}–46^{10} kehtetuks tunnistamine. Kuna eelnõuga lisandub vastutuse peatükki uus paragrahv uue koosseisuga, tunnistatakse kehtetuks paragrahvid, mis oma sisult peavad olema vastutuse peatüki kolm kõige viimast paragrahvi – paragrahv, mis selgitab, kuidas määrata juriidilise isiku ja konsolideerimisgrupi käivet trahvi suuruse arvutamisel, paragrahv väärtegude aegumise kohta ning paragrahv väärtegude menetleja kohta. Paragrahvid sätestatakse uuesti §-des 51^{1}–51^{3}.

EVKS uus § 46^{11}. Seadust täiendatakse uue karistusnormiga, mida FI saab rakendada DORA määruses sätestatud nõuete rikkumise korral. Nimelt on DORA määruse artikli 50 lõikes 3 sätestatud, et liikmesriigid kehtestavad õigusnormid, milles sätestatakse asjakohased halduskaristused ja parandusmeetmed määruse rikkumise puhuks, ning tagavad nende tulemusliku rakendamise. Sama artikli lõike 4 punktis c on sätestatud, et liikmesriigid annavad pädevatele asutustele õiguse võtta mis tahes liiki meetmeid, sealhulgas rahalisi meetmeid, tagamaks, et finantssektori ettevõtjad jätkavad õigusnormide järgimist. Eelnõuga nähakse ette, et füüsilise isiku korral on võimalik karistada rahatrahviga kuni 5 000 000 eurot või kuni kahekordse väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas ning juriidilise isiku korral karistatakse rahatrahviga kuni 5 000 000 eurot või kuni kahekordse väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas või kuni kümme protsenti juriidilise isiku või tema konsolideerimisgrupi konsolideeritud käibest.

Uue paragrahvi lõike 1 sõnastuses on viidatud järgmistele DORA määruse nõuete rikkumistele:
- art 5–14: IKT- riski juhtimine;
- art 16–18, art 19 lõiked 1–5: IKT intsidentide haldamine ja liigitamine ning nendest teavitamine;
- art 24, 25, art 27 lõiked 1–8: digitaalse tegevuskerksuse testimine;
- art 28 lõiked 1–8, art 29, art 30 lõiked 1–4: kolmandast isikust tuleneva IKT-riski juhtimine;
- art 42 lg 3: kolmanda isikuga seotud riskide arvesse võtmine.

EVKS uued paragrahvid. Kehtetuks tunnistatud §-d 46^{8}–46^{10} sätestatakse uuesti §-des 51^{1}–51^{3}.

3.10. Eelnõu § 10. Väärtpaberituru seaduse muutmine

VpTS § 1 lõike 2 muutmine. DORA määruse kohaldamisalasse kuuluvad mh ühisrahastusteenuse osutajad, kes on määratletud Euroopa Parlamendi ja nõukogu määruse (EL) 2020/1503 (35) artikli 2 lõike 1 punktis e. Lõike 2 sõnastust täiendatakse viitega VpTS uuele §-le 237^{90} ehk karistusi DORA määruse nõuete rikkumise eest kohaldatakse ka viidatud ühisrahastusteenuse osutajatele.

VpTS § 10[1] muutmine (ei ole seotud DORA ülevõtmisega, seaduses parandatakse EL määruse nimetus õigeks)**.** Euroopa Parlamendi ja Nõukogu määrusega (EL) 2019/2033, 27. november 2019, mis käsitleb investeerimisühingute suhtes kohaldatavaid usaldatavusnõudeid ning millega muudetakse määrusi (EL) nr 1093/2010, (EL) nr 575/2013, (EL) nr 600/2014 ja (EL) nr 806/2014, muudeti Euroopa Parlamendi ja nõukogu määruse (EL) nr 575/2013 pealkirja, mistõttu viiakse VpTS-is olev viide määrusele kooskõlla selle õige nimetusega.

VpTS § 66 lõike 2 punkti 5 ja § 70[1] lõike 3 punkti 5 muutmine ning uued punktid (ei ole seotud DORA direktiiviga, kuid on tehniline muudatus, et vältida seaduses olevat tühja viidet). Kuna ÄS § 386 lõike 2 punkt 4 on tunnistatud kehtetuks, korrigeeritakse VpTS sõnastust ja kustutatakse viide kehtetule ÄS punktile 4. ÄS-ist välja jäetud punkt sõnastatakse VpTS-is. Seega peab kolmanda riigi investeerimisühing Eestis filiaali asutamise loa või piiriülese teenuse osutamise loa taotlemisel esitama FI-le äriühingu põhikirja või ühingulepingu asukohamaa seaduste kohaselt tõestatud ärakirja, kui põhikirja või ühingulepingu registrile esitamine on nõutav ka ühingu asukohamaal.

VpTS § 81[1] täiendamine uue lõikega 4[1]. Paragrahv reguleerib investeerimisühingu üldisi organisatsiooninõudeid. Muudatusega nähakse ette investeerimisühingu kohustus rakendada mh DORA määrust.

VpTS § 82[6] lõike 4 muutmine. Paragrahv reguleerib olulise tööülesande või tegevuse edasiandmist, sealjuures on olulised tööülesanded ja tegevused määratletud komisjoni delegeeritud määruse (EL) nr 2017/565 artiklis 30. Muudetava lõike 4 kohaselt peab olulise tööülesande või tegevuse edasiandmisel olema selles delegeeritud määruses sätestatud nõuded. Lõike sõnastusse lisatakse viide DORA määrusele ehk info- ja kommunikatsioonitehnoloogia teenuse edasiandmisel tuleb mh täita DORA määruses ette nähtud edasiandmise nõudeid (lisaks määruses (EL) nr 2017/565 sätestatule).

VpTS § 82[15] lõike 1 teise lausesse lisatakse viide DORA määrusele. Lõike 1 esimene lause ütleb, et algoritmkauplemisega tegelemisel, sealhulgas algoritmipõhise välkkauplemistehnika kasutamisel, rakendab investeerimisühing oma äritegevuse jaoks sobivaid ja tõhusaid süsteeme ning riskikontrolli, tagamaks, et algoritmkauplemiseks kasutatav infotehnoloogiline süsteem on töökindel ja piisava võimsusega, selles rakendatakse asjakohaseid kauplemiskünniseid ja -piirmäärasid ning see ennetab ekslike korralduste andmist ja muid toiminguid, mis võivad ohustada väärtpaberituru korra- või õiguspärast toimimist. Sama lõike teises lauses on sätestatud, et investeerimisühing järgib selliste meetmete rakendamisel muu hulgas komisjoni delegeeritud määruses (EL) nr 2017/589 sätestatut. Muudatusega lisatakse viide lisaks DORA määrusele.

VpTS § 82[15] lõike 5 sõnastuses on täpsustatud, et talitluspidevuse kord sisaldab muu hulgas info- ja kommunikatsioonitehnoloogia talitluspidevuse põhimõtteid ja plaane, aga ka info- ja kommunikatsioonitehnoloogia reageerimis- ja taasteplaane. Lõike teise lausesse on lisatud viide DORA määruse peatükkidele 2 ja 4, mis reguleerivad info- ja kommunikatsioonitehnoloogia riskide juhtimist, sealhulgas nõudeid info- ja kommunikatsioonitehnoloogiale, protokollidele ja vahenditele, ning digitaalse tegevuskerksuse testimist.

Tõhusaid talitluspidevuse ja taasteplaane on vaja selleks, et investeerimisühing saaks kohe ja kiiresti lahendada IKT intsidendid, eelkõige tulla toime küberrünnetega, piirates kahju ja seades prioriteediks tegevuse jätkamise ja taastemeetmed kooskõlas oma varunduspõhimõtetega.

Sealjuures ei tohiks selline tegevuse jätkamine kuidagi seada ohtu võrgu- ja infosüsteemide terviklust ja turvalisust või andmete kättesaadavust, autentsust, terviklust ja konfidentsiaalsust.

Investeerimisühing testib kõiki funktsioone toetavate IKT-süsteemide IKT talitluspidevuse plaane ning IKT reageerimis- ja taasteplaane vähemalt kord aastas ja kriitilise tähtsusega või olulisi funktsioone toetavate IKT-süsteemide oluliste muudatuste korral. Sealjuures lisatakse testimisplaanidesse stsenaariumid, mis käsitlevad küberründeid ja esmase IKT-taristu ja varuvõimsuse vahelist ümberlülitust, varundamist ja varurajatisi.

VpTS uus § 82[18]. DORA määruse artikli 19 lõike 1 kohaselt peab finantsasutus teavitama pädevat asutust tõsistest IKT-ga seotud intsidentidest. Lisaks annab määrus liikmesriigile võimaluse ette näha, et mõned või kõik finantssektori ettevõtjad esitavad pädevale asutusele või küberturbe intsidentide lahendamise üksustele, mis on määratud või loodud direktiivi (EL) 2022/2555 kohaselt, ka esialgse teate ja kõik raportid, kasutades DORA määruse artiklis 20 osutatud vorme. Lõikega 1 nähakse ette, et investeerimisühing teavitab lisaks FI-le ka RIA-t.

Intsidentide liigitamise kriteeriumid on ette nähtud DORA määruse artikli 18 lõikes 1, kuid täpsemad kriteeriumid tõsiste intsidentide määratlemiseks töötavad välja ESA-d koostöös EKP ja ENISA-ga.

Lisaks sätestab DORA määruse artikli 19 lõige 2, et finantsasutused võivad vabatahtlikult teatada asjaomasele pädevale asutusele olulistest küberohtudest, kui nad peavad ohtu finantssüsteemi, teenusekasutajate või klientide jaoks oluliseks, sealjuures võivad liikmesriigid otsustada, et need finantsasutused, kes teatavad vabatahtlikult esimese lõigu kohaselt, võivad kõnealuse teate edastada ka direktiivi (EL) 2022/2555 kohaselt määratud või loodud küberturbe intsidentide lahendamise üksustele (lõige 3).

VpTS § 114 muutmine. Muudatuse kohaselt ei ole investeerimisühingu piiriülene ümberkujundamine lubatud. Muudatuse eesmärk on tagada Eesti investorite parem kaitse. Arvestades finantssektori erisusi, ei ole praktikas finantsasutuse ümberkujundamine võrreldav nn tavalise äriühingu ümberkujundamise protsessiga.

VpTS § 119[17] uus lõige 3. Kuna DORA määruse kohaldamisalasse kuuluvad mh aruandlusteenuse osutajad, on liikmesriigi valikukoha (artikli 19 lõiked 1 ja 2) rakendamiseks vajalik ka nende puhul täpsustada, et intsidentidest ja küberohtudest tuleks teavitada ka RIA-t. Aruandlusteenuse osutajatele kohaldatakse investeerimisühingu kohta sätestatut.

VpTS § 121 lõikes 3 tehakse terminoloogiline muudatus, asendades sõna „infotehnoloogiliste“ terminiga „info- ja kommunikatsioonitehnoloogiliste“.

VpTS § 124[6] lõigete 1 ja 3 muutmine. Paragrahv 124[6] reguleerib, millised organisatsioonilised nõuded kohalduvad reguleeritud turu korraldajale. Kui lõikes 1 on sätestatud, et korraldaja kehtestab õiguslikud, tehnilised ja organisatsioonilised meetmed ja rakendab neid, et tuvastada ja maandada turu õigus- ja korrapärase toimimise riskid, siis muudatusega lisatakse loetelusse ka info- ja kommunikatsioonitehnoloogia riskid, mille juhtimisel järgitakse DORA määruse teises peatükis sätestatut.

VpTS § 124[6] lõike 3 muutmine. DORA direktiiv näeb ette, et direktiivi 2014/65/EL artikli 47 lõike 1 punkt c kustutakse, kuna vastav säte on juba kaetud DORA määrusega. VpTS-is on vastav säte § 124[6] lõikes 3. Kuna samas sättes on defineeritud kauplemissüsteem, on eelnõus otsustatud seda sätet mitte kustutada, vaid lisada sinna viide DORA määrusele.

VpTS § 125[1] lõike 2 muudatus näeb ette, et korraldaja kehtestab teenuse osutamise jätkuvuse tagamiseks muu hulgas info- ja kommunikatsioonitehnoloogia talitluspidevuse põhimõtted ja plaani ning info- ja kommunikatsioonitehnoloogia reageerimis- ja taasteplaanid.

VpTS § 125[2] lõike 1 muutmine. Paragrahv reguleerib organisatsioonilisi lisanõudeid elektroonilisel kauplemisel. Muudetava lõike esimeses lauses asendatakse termin „infotehnoloogilistest süsteemidest" terminiga „info- ja kommunikatsioonitehnoloogilistest süsteemidest". Lõike teise lausesse lisatakse viide DORA määruse peatükkidele II ja IV ehk korraldaja nõuab turul osalejalt algoritmide asjakohast testimist ja selleks vajaliku keskkonna loomist vastavalt DORA määruses sätestatule.

VpTS uus § 125[3]. DORA määruse artikli 19 lõike 1 kohaselt peab finantsasutus teavitama pädevat asutust tõsistest IKT-ga seotud intsidentidest. Lisaks annab määrus liikmesriigile võimaluse ette näha, et mõned või kõik finantssektori ettevõtjad esitavad pädevale asutusele või küberturbe intsidentide lahendamise üksustele, mis on määratud või loodud direktiivi (EL) 2022/2555 kohaselt, ka esialgse teate ja kõik raportid, kasutades DORA määruse artiklis 20 osutatud vorme (lõiked 1 ja 2). Lõikega 1 nähakse ette, et korraldaja teavitab lisaks FI-le ka RIA-t.

Intsidentide liigitamise kriteeriumid on ette nähtud DORA määruse artikli 18 lõikes 1, kuid täpsemad kriteeriumid tõsiste intsidentide määratlemiseks töötavad välja ESA-d koostöös EKP ja ENISA-ga.

Lisaks sätestab DORA määruse artikli 19 lõige 2, et finantsasutused võivad vabatahtlikult teatada asjaomasele pädevale asutusele olulistest küberohtudest, kui nad peavad ohtu finantssüsteemi, teenusekasutajate või klientide jaoks oluliseks, sealjuures võivad liikmesriigid otsustada, et need finantsasutused, kes teatavad vabatahtlikult esimese lõigu kohaselt, võivad kõnealuse teate edastada ka direktiivi (EL) 2022/2555 kohaselt määratud või loodud küberturbe intsidentide lahendamise üksustele (lõige 3).

VpTS § 163[1] lõike 7 muutmine. Sättesse lisatakse viide uuele VpTS §-le 125[3]. Lõige reguleerib, milliseid turu korraldaja suhtes kohalduvaid sätteid kohaldatakse mitmepoolse kauplemissüsteemi ja organiseeritud kauplemissüsteemi korraldajale.

VpTS § 230 lõike 1 täiendamine uue punktiga. Paragrahv reguleerib FI õigusi ja ülesanded, sealjuures on lõikes 1 loetelu EL õigusaktidest, milles sätestatu täitmise üle FI järelevalvet teostab. Sellesse loetelusse lisatakse viide ka DORA määrusele ehk FI teostab järelevalvet muu hulgas DORA määruses sätestatu üle.

VpTS § 230 uus lõige 7. FI peab avalikustama DORA määruse artikli 50 kohaselt võetud meetmete alusel tehtud otsuse kohta teate oma veebilehel nagu on sätestatud artiklis 54.

Näiteks on FI-l õigus tutvuda kõigi dokumentidega või mis tahes vormis muude andmetega, mis võiksid olla FI ülesannete täitmiseks olulised, ja saada või teha nende dokumentide koopiaid, teha kohapealsed kontrolle või uurimisi ning nõuda määruse nõuete rikkumise korral parandus- ja ennetusmeetmete võtmist.

DORA määruse artikli 50 lõige 4 kohustab liikmesriike pädevatele asutustele andma õiguse kohaldada määruse nõuete rikkumise korral halduskaristusi või parandusmeetmeid. Sellisteks meetmeteks on:

- ettekirjutuse tegemine, et füüsiline või juriidiline isik lõpetaks rikkuva tegevuse ja hoiduks selle tegevuse kordamisest;

- sellise tegevuse või tava peatamise nõudmine, mis on vastuolus määruse sätetega;
- mis tahes liiki meetmete võtmine, sealhulgas rahaliste meetmete, tagamaks, et finantsasutused jätkavad õigusnormide järgimist;
- liikmesriigi õigusega lubatud ulatuses sideoperaatorite valduses olete andmeliiklusandmete nõudmine, kui on piisav alus kahtlustada määruse nõuete rikkumist ja kui sellised andmed võivad olla olulised määruse rikkumiste uurimisel, ning
- avalike teadaannete väljastamine, mis sisaldavad füüsilise või juriidilise isiku identiteeti ja rikkumise laadi.

Et võetud meetmetel oleks hoiatav mõju laiemale avalikkusele, näeb määrus ette rikkumist puudutavate otsuste ja rakendatud meetmete avalikustamise. DORA määruse artikli 54 lõike 1 kohaselt avaldavad pädevad asutused oma ametlikel veebisaitidel põhjendamatu viivituseta kõik halduskaristuse määramise otsused, mida ei ole edasi kaevatud pärast seda, kui karistuse saanud isikut on otsusest teavitatud. Avaldada tuleb teave rikkumise liigi ja laadi kohta, vastutavad isikud ning määratud karistused. Erandiks on olukorrad, kus juriidilise isiku nime või füüsilise isiku nime ja isikuandmete avaldamine oleksid ebaproportsionaalsed või nende andmete avaldamine ohustaks finantsturgude stabiilsust või pooleli olevat uurimist (eelkõige mõeldud järelevalve- ja väärteomenetlust, kuid võib hõlmata ka kriminaalmenetlust tegevusloata tegutsemise puhul) või põhjustaks asjaomasele isikule ebaproportsionaalselt suurt kahju. Sellisel puhul võib avaldamise edasi lükata, jätta isikuid puudutav teave avaldamata või loobuda sellise kaasuse kohta teabe avaldamisest üldse.

VpTS uus § 237[90]. Seadust täiendatakse uue karistusnormiga, mida FI saab kohaldada DORA määruses sätestatud nõuete rikkumise korral. Nimelt on DORA määruse artikli 50 lõikes 3 sätestatud, et liikmesriigid kehtestavad õigusnormid, milles sätestatakse asjakohased halduskaristused ja parandusmeetmed määruse rikkumise puhuks, ning tagavad nende tulemusliku rakendamise. Sama artikli lõike 4 punktis c on sätestatud, et liikmesriigid annavad pädevatele asutustele õiguse võtta mis tahes liiki meetmeid, sealhulgas rahalisi meetmeid, tagamaks, et finantssektori ettevõtjad jätkavad õigusnormide järgimist. Eelnõuga nähakse ette, et füüsilise isiku korral on võimalik karistada rahatrahviga kuni 5 000 000 eurot või kuni kahekordse väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas ning juriidilise isiku korral karistatakse rahatrahviga kuni 5 000 000 eurot või kuni kahekordse väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas või kuni kümme protsenti juriidilise isiku või tema konsolideerimisgrupi konsolideeritud käibest

Uue paragrahvi lõike 1 sõnastuses on viidatud järgmistele DORA määruse nõuete rikkumistele:
- art 5–14: IKT- riski juhtimine;
- art 16–18, art 19 lõiked 1–5: IKT intsidentide haldamine ja liigitamine ning nendest teavitamine;
- art 24, 25, art 27 lõiked 1–8: digitaalse tegevuskerksuse testimine;
- art 28 lõiked 1–8, art 29, art 30 lõiked 1–4: kolmandast isikust tuleneva IKT-riski juhtimine;
- art 42 lg 3: kolmanda isikuga seotud riskide arvesse võtmine.

VpTS § 237[89] kehtetuks tunnistamine ja uus § 262[3]. Muudatus on tehniline, menetluse paragrahvi asukoht muutub.

Seaduse normitehniline märkuse. Muudatusega lisatakse viide DORA direktiivile.

Eelnõu § 11. Seaduse jõustumine.

DORA nõuete rakendamiseks vajalikud seadusemuudatused jõustusvad 17. jaanuaril 2025. aastal. Ülejäänud muudatused jõustusvad tavakorras.

4. TERMINOLOOGIA

Eelnõuga võetakse kasutusele järgmised uued terminid:

- digitaalne tegevuskerksus (DORA määruse artikli 3 punkt 1) – finantssektori ettevõtja suutlikkus luua, tagada ja vaadata läbi oma tegevuse terviklikkust ja usaldusväärsust, tagades kas otseselt või kaudselt kolmandast isikust IKT-teenuste osutajate pakutavate teenuste kasutamise kaudu kogu IKTga seotud suutlikkuse, mida on vaja selliste võrgu- ja infosüsteemide turvalisuse käsitlemiseks, mida finantssektori ettevõtja kasutab ning mis toetavad finantsteenuste jätkuvat osutamist ja nende kvaliteeti, sealhulgas katkestuste vältel;
- võrgu- ja infosüsteemid (DORA määruse artikli 3 punkt 2) – NIS2 direktiivi artikli 6 punktis 1 määratletud võrgu- ja infosüsteem. NIS2 direktiiv omakorda määratleb, et võrgu- ja infosüsteem on (a) direktiivi (EL) 2018/1972 artikli 2 punktis 1 määratletud elektroonilise side võrk; (b) seade või omavahel ühendatud või seotud seadmete rühm, millest vähemalt ühes toimub mõne programmi kohaselt digiandmete automaatne töötlemine, või (c) digiandmed, mida salvestatakse, töödeldakse, saadakse päringutega või edastatakse punktidega a ja b hõlmatud komponente kasutades nende töö, kasutamise, kaitsmise või hooldamise jaoks;
- tõsine IKT-ga seotud intsident – IKT-ga seotud intsident, millel on suur negatiivne mõju võrgu- ja infosüsteemidele, mis toetavad finantssektori ettevõtja kriitilise tähtsusega või olulisi funktsioone;
- oluline kübeoht – küberoht, mille tehnilised tunnused näitavad, et selle tulemuseks võib olla IKTga seotud oluline intsident või tegevust või turvalisust mõjutav maksetega seotud oluline intsident;
- IKT-teenus – digi- ja andmeteenus, mida osutatakse pidevalt IKT-süsteemide kaudu ühele või mitmele sise- või väliskasutajale, sealhulgas riistvara teenusena ja riistvarateenused, mis hõlmab tehnilise toe pakkumist riistvara pakkuja tarkvara- või püsivarauuenduste kaudu, välja arvatud tavapärased analoogtelefoniteenused;

5. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu on kooskõlas Euroopa Liidu õigusega (vt seletuskirja lisas esitatud tabelit DORA direktiivi ja DORA määruse vastavuse kohta).

6. Seaduse mõjud

6.1. Mõju finantsasutustele

Sihtrühma suurus. FI tegevusloa ja registreeringu alusel tegutsevad finantsasutused (vt seletuskirja punkti 2.4).

Mõju majandusele	
Mõju ulatus ja avaldumise sagedus	DORA määrus näeb ette finantsasutusele üsna detailsed digitaalse tegevuskerksuse tagamise reeglid. Operatsiooniliste riskide, sealhulgas IKT riskide juhtimise nõuded, sealhulgas nõuded küberturvalisuse tagamiseks, ei ole finantssektori jaoks midagi uut. Määrusega kehtestatavad nõuded on juba kaetud erinevate standardite, seaduste ja suunistega: ISO27000 standardid, küberturvalisuse seadus, hädaolukorra seadus ja FI juhendid (nt nõuded finantsjärelevalve subjekti infotehnoloogia ja infoturbe korraldusele), EBA suunis pankade IKT ja turvariskide juhtimiseks, EIOPA suunis pilveteenuseosutajatele tegevuse

	edasiandmise kohta ja SSM järelevalve). Lisaks on eurosüsteemis välja töötatud *Cyber Resilience Oversight Expectations*. Kuigi suuremad ja keerukamad finantsasutused juba omavad keerulisi IKT-süsteeme ja protseduure, tähendab ka nende läbivaatamine ja DORA nõuetega kooskõlla viimine halduskoormuse tõusu. Võib väita, et digitaalse tegevuskerksuse nõuete rakendamiseks peavad finantsasutused teatud ümberkorraldusi tegema (nt juhtimisstruktuuri arendamine), mis eeldab rahaliste vahendite kaasamist. Samas on DORA üheks oluliseks põhimõtteks, et finantsasutused peaksid IKT-riski juhtimise raamistiku rakendamiseks ressursside ja suutlikkuse jaotamisel võtma oma IKT-ga seotud vajaduste puhul igakülgselt arvesse oma suurust ja üldist riskiprofiili ning oma teenuste, tegevuse ja toimingute laadi, ulatust ja keerukust. Seega ka kulud peaks olema proportsioonis asutuse suuruse ja tegevuse laadiga. Üldine vastutus IKT riskijuhtimise raamistiku ja muude DORA kehtestatud juhtimiskohustuste eest lasub finantsasutuse juhtkonnal, kes vastutab raamistiku ülevaatamise, heakskiitmise, rakendamise ja ajakohastamise eest. Ainuüksi esmase küberhügieeni järgimine aitab minimeerida finantsasutuse äriprotsesside katkestuste mõju ning hoida ära majandusele suurte kulude tekkimist. Finantsinspektsiooni 2022. aasta aastaraamatus[35] on välja toodud, et 2022. aastal teavitasid pangad ja makseasutused Finantsinspektsiooni olulisest IT-intsidendist kokku 65 korral, küberrünnakute põhjustatud juhtumeid oli üheksa. Sõltumata rünnete sagenemisest ei õnnestunud nendega märkimisväärseid kahjusid pankadele tekitada ega segadust põhjustada. Pangad olid rünnakute tõrjumiseks hästi valmistunud. Digitaalse tegevuskerksuse baastestimise nõuded kohalduvad kõikidele finantsasutustele, mistõttu ettevõtjad, kellele varasemalt ei ole analoogsed nõuded kohaldunud või neid pole sisekorrareeglites ette nähtud, peavad oma süsteemid ja protsessid viima vastavusse mh testimise nõuetega. Kõrgemad testimise nõuded (süvastestimine) kohalduvad olulistele ja kübervõimekatele teenuseosutajatele (näiteks suured, süsteemselt olulised ja IKT seisukohast küpsed krediidiasutused, börsid, väärtpaberite keskdepositooriumid ja kesksed vastaspooled). Seega võib väita, et süvatestide tegemisega kaasnev halduskoormuse tõus ja rahaliste kulude suurenemine mõjutab siiski väikest, aga olulist osa finantssektorist. Kuna ohuteabel põhineval läbistustestimisel tuleb üldjuhul kasutada välistestijaid/ekspertrühmasid (sisetestijad on lubatud teatud tingimustel ja vaid pädeva asutuse nõusolekul), siis see tähendab ettevõtja jaoks

[35] https://www.fi.ee/sites/default/files/2023-04/Finantsinspektsiooni%20aastaraamat%202022_0.pdf

	samuti märkimisväärseid kulusid. Kulud võivad varieeruda sõltuvalt ettevõtte suurusest, tegevusvaldkonnast, turvameetmete tasemest, keerukusest, testimise ulatusest jne. Kuigi kulud võivad olla märkimisväärsed, on see oluline investeering ettevõtte turvalisuse tagamiseks ja võimalike kahjude, sealhulgas mainekahju, ennetamiseks. Kõikidele finantsasutustele kohalduvad ka IKT-teenuse edasiandmise nõuded. Kuivõrd finantssektoris kehtivad õigusaktid ja suunised hõlmavad samuti nõudeid teenuste edasiandmisele (sealjuures ESA-de suunised), siis peavad finantsasutused juba käesoleval hetkel järgima EL õigusest tulenevaid nõudeid teenuste edasiandmisele. Samas võib DORA määruse kohaldamine tähendada, et senised IKT teenuseosutajad ei sobi enam teenuseosutajaks ja finantsasutus peab leidma partneri, kellega seotud kulud võivad olla suuremad kui seni oli arvestatud. Vabatahtlik teabevahetus küberohtudest teiste finantsasutustega võib tähendada küll halduskoormuse tõusu, kuid kogemuste vastastikune jagamine võib ära hoida uusi intsidente ja kulusid ettevõttele. Kuna tegemist on vabatahtlikkusel põhineva sättega, siis ei saa sellega seotud mõju pidada ka oluliseks. Digitaalse tegevuskerksuse nõuete järgmine on pidev. Suurem mõju avaldub IKT-riskide juhtimise raamistiku väljatöötamisel, digitaalse tegevuskerksuse testimisel, eriti süvatestimisel, ning oluliste IKT-ga seotud intsidentide haldamisel.
Ebasoovitavate mõjude avalumise risk	Ebasoovitavate mõjude avalumise risk võib esineda olukorras, kui vaatamata digitaalse tegevuskerksuse nõuete järgimisele ei õnnestu IKT-ga seotud tõsiseid intsidente ära hoida, mis võib omakorda ettevõtjas kaasa tuua ärikatkestusi või tõrkeid kriitiliste funktsioonide toimimisel, mis omakorda võib tähendada ettevõttele rahalist kahju. Halvimal juhul saavad küberrünnete toimepanijad finantsasutuse kaudu rahalist tulu, tuues sellega ettevõtja jaoks kaasa märkimisväärsed majanduslikud tagajärjed. Samuti võib ettevõtja reputatsioon kannatada ja ettevõtja võib jääda ilma hetke ja potentsiaalsetest klientidest. Seega jääb alati ülesse risk, et vaatamata küberkerksuse nõuete rakendamisele, on küberründajad ettevõtjatest kaks sammu ees. Lisaks võib ebasoovitav mõju avalduda juhul, kui IKT-teenuseosutaja või temaga seotud leping ei vasta õigusaktist tulenevale nõudele, mistõttu tuleb teenuseosutaja välja vahetada. Ka IKT teenuseosutaja maksejõuetuks muutumine või tegevuse katkemine võib avaldada finantsasutustele süsteemset mõju. Samas ei pruugi teatud teenuseosutajad olla hõlpsasti asendatavad. Seetõttu ongi oluline, et kriitilisi ja olulisi funktsioone toetavad IKT-teenuse lepingud sisalduksid ka väljumisstrateegiaid sellise riski maandamiseks.
Mõju olulisus	Keskmine mõju, arvestades, et finantsasutused rakenduvad juba hetkel toimepidevuse nõudeid.
Sotsiaalne mõju	

	Sõltub finantsasutusest, kas asutuse juhtimiskorralduses on vaja teha muudatusi seoses uute isikute tööle värbamisega. Määrusega on ette nähtud IKT-turbe teadlikkuse suurendamise programmid ja digitaalse tegevuskerksuse koolitused, edendamaks ettevõtja igal tasandil kõigi töötajate suurt teadlikkust küberriskidest ja pühendumust tagada kõigil tasanditel range küberhügieen.

6.2. Mõju investoritele ja finantsteenuste klientidele

Sihtrühma suurus. Sihtrühma suurust klientide arvu mõttes on käesoleval hetkel keeruline hinnata, kuid arvestades, et ainuüksi arvelduskonto on Eestis 98%-l täisealisest elanikkonnast, võib väita, et potentsiaalse sihtrühma suurusega on hõlmatud peaaegu kogu Eesti täisealine elanikkond.

Majanduslik mõju	
Mõju ulatus ja avaldumise sagedus	Kuna finantsasutused arendavad nõuetele tuginedes IKT-suutlikkust ja üldist kerksust, et tulla toime tegevuse katkestustega, aitab see säilitada EL finantsturgude stabiilsust ja usaldusväärsust ning seega tagada investorite ja tarbijate kaitse kõrge taseme. Nõuete rakendamine aitab kaitsta nii teabevara klientide kohta kui ka klientide rahalisi vahendeid. Klientide usaldus, et nende andmed on kaitstud, tõuseb.
Ebasoovitavate mõjude avalumise risk	Sõltub ilmselt finantsasutusest, kas uutele nõuetele vastavuse tagamine eeldab niivõrd suuri ressursse, et see võiks mõjutada ka finantsteenuse hinda (ehk teenus muutub kliendi jaoks kallimaks).
Mõju olulisus	Klientide kaitse on alati olulise mõjuga, kuid klientide enda halduskoormus seoses eelnõuga ei tõuse, samuti ei tohiks eelnõu rakendamine mõjutada teenuse hindasid. Kokkuvõttes on mõju klintidele positiivne, kuna DORA nõuded tagavad kõrgemad turvastandardid ning klientide andmete ja vara parema kaitse.
Sotsiaalne mõju	
	Kui finantsasutus ei suuda tagada küberkerksuse kõrget taset, siis mustema stsenaariumi kohaselt võivad küberründed olla finantsteenuste klientidele selliste tagajärgedega, et need võivad mõjutada ka klientide toimetulekut rahaliselt.

6.3. Mõju kriitilise tähtsusega kolmandast isikust IKT-teenuseosutajatele

Sihtrühma suurus. Sihtrühma kuuluksid IKT teenuseosutajad, kes on Euroopa mõistes suured, osutades teenust mitmes liikmesriigis ja suurele hulgale finantsasutustele, sealjuures võetakse nende määratlemisel arvesse pakutavate teenuste süsteemset mõju ja iseloomu ning finantsasutuste sõltuvust nende osutatavatest teenustest. Kriitilise tähtsusega IKT teenuseosutaja määratlemiseks kehtestatakse lisaks DORA määruse üldisematele kriteeriumitele alamakt ning lõpliku otsuse, millised ettevõtjad on kriitilised selle määratluse alusel ja hakkaksid kuuluma EL-ülese järelevaatamise alla, teevad ESA-d.

Pigem võiks eeldada, et ükski Eesti IKT teenuseosutaja sihtrühma ei kuulu.

Mõju ulatus ja avaldumise sagedus	ESA-d hakkavad teostama Euroopaülest järelevaatamist kriitilise tähtsusega ITK teenuseosutajate üle ning sellega kaasnevaid kulusid rahastataks täielikult kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatele kehtestatud tasudest. Seega tähendab uus regulatsioon rahalisi kulusid ainuüksi tasude näol.
Ebasoovitavate mõjude avalumise risk	Kui teenuseosutaja ei ole teavitanud juhtivat järelevalveasutust, kas ta järgib talle tehtud soovitust või mitte või kui teenuseosutaja selgitus ei ole piisav selle kohta, miks ta ei järgi soovitust, siis avaldatakse sellised juhud. Avaldatud teabes avalikustatakse sellise IKT-teenuseosutaja identiteet ning teave nõuete täitmata jätmise liigi ja laadi kohta.
Mõju olulisus	Arvestades, et ilmselt ükski Eesti ettevõtja kriitilise tähtsusega IKT teenuseosutaja määratluse alla ei lähe, mõju puudub.

6.4. Mõju järelevalve- ja riiklikele asutustele

Sihtrühma suurus:

- 2022. aasta lõpu seisuga on FI-s 127 töötajat.
- RIA-s on ligemale 250 töötajat.

Majanduslik mõju	
Mõju ulatus ja avaldumise sagedus	**Finantsinspektsioon** Kavandatavad muudatused mõjutavad FI järelevalvelist tegevust, kuna FI on DORA määruse artikli 46 kohaselt pädev asutus, kes teostab järelevalvet digitaalse tegevuskerksuse nõuete täitmise üle. Järelevalve teostamine eeldab spetsiifilisi teadmisi IKT riskidest, süsteemidest, vahenditest jne. Sealjuures peab FI-s olema kompetents, et hallata teavitusi, mida finantsasutused FI-le edastavad seoses tõsiste IKT intsidentidega. Järelevalve on pidev. Samas FI valmisolek teostada DORA määruse nõuete üle järelevalvet on juba käesoleval hetkel väga hea. Finantsinspektsiooni 2022. aasta aastaraamatus on kirjas, et „Finantsinspektsioon hindab oma järelevalvetegevuse käigus muu hulgas pankade IT-organisatsiooni, IT-struktuuri ja haldust, talitluspidevust, arendustöid, turvalisust ja küberriskide juhtimist tervikuna. Finantsinspektsioon analüüsib regulaarse aruandluse põhjal kõiki olulisi intsidente, vajadusel küsib pankadelt tegevuskavasid ning jälgib, et rakendataks meetmeid, mis aitavad tulevikus sarnaste intsidentide kordumist vältida. Inspektsioon koostab valdkonnaüleseid IT- ja küberriskianalüüse, mille põhjal tuvastab suure IT-riskiga finantssektori osad. Suurte IT-riskidega pangad peavad välja töötama tegevuskavad, mida Finantsinspektsioon jälgib eriaruandluse korras. Lähtuvalt riskidest analüüsib inspektsioon detailsemaid teemasid – aastal 2022 oli fookus pankade küberriskide haldusel ja maandamisel ning IT turvatestimiste protsessi toimimisel.“ Seoses EL-ülese järelevaatamisega kriitilise tähtsusega IKT teenuseosutajate üle, peab FI kõrgetasemeline esindaja kuuluma järelevaatamise foorumisse. Lisaks on FI esindaja kontrollrühma liige, kui Eesti finantsasutusele osutab teenust kriitilise tähtsusega IKT-

	teenuseosutaja ning selle teenuseosutaja jaoks on moodustatud juhtivat järelevalveasutust abistav kontrollrühm. Viidatud rühmitustes osalemine eeldab rahaliste vahendite suurendamist. Kuna ESA-de DORA määruse rakendamiseks vajalike IKT-süsteemide arendamist rahastatakse esialgu liidu ja riiklike pädevate asutuste osamaksetest (hiljem kaetakse püsikulud kriitliste IKT-teenuseosutajate enda tasudest), tähendab see algusperioodil lisakulusid ka FI-le (sealjuures FI eelarve moodustub 93% ulatuses finantsjärelevalve subjektide tasudest). **Riigi Infosüsteemi Amet** Koostöö FI-ga ja tehnilise nõu andmine, kui FI seda vajab, võib tähendada halduskoormuse tõusu (mõju riigieelarvele), kuid eeldatavasti on sellisest koostööst saadav kasu proportsioonis sellele kuluva ressurssiga. Kuna finantsasutuste teavitused tõsiste IKT intsidentide kohta jõuavad ka RIA-ni, aitab see suurendada ameti teadlikkust finantsasutuste küberintsidentidest ning hõlbustada asjakohastel juhtudel viivitamatu abi osutamist neile.
Ebasoovitavate mõjude avalumise risk	Ebasoovitavate mõjude avalumise riski ei tuvastatud.
Mõju olulisus	Mõju võib pidada keskmiseks.
Sotsiaalne mõju	
	Võib osutada vajalikuks uue töökoha või töökohtade loomine FI-s ja personali täiendkoolitamine DORA-st tulenevate ülesannete täitmiseks.

6.5. Muud mõjud

Regulatsioonil puudub mõju riigi julgeolekule ja välissuhetele, elu- ja looduskeskkonnale ning regionaalarengule.

DORA määruse artikli 1 lõike 3 kohaselt ei piirata DORA määrusega liikmesriikide vastutust seoses riigi põhifunktsioonidega avaliku julgeoleku, riigikaitse ja riikliku julgeoleku tagamisel kooskõlas liidu õigusega.

6.6. Mõjude kokkuvõte

Halduskoormus finantsasutustele. Ettevõtjate halduskoormus suureneb, kuid sõltuvalt ettevõtjas on see mõju erinev.

Halduskoormuse klientidele. Eelnõu ei mõjuta finantsteenuste klientide halduskoormust.

Halduskoormus avalikule sektorile. Avaliku sektori halduskoormus võib suureneda, seda eelkõige seoses koostöö tõhustamisega FI ja RIA vahel.

7. Seaduse rakendamisega seotud riigi ja kohaliku omavalitsuse tegevused, eeldatavad kulud ja tulud

Seaduse rakendamisega ei kaasne tulusid riigieelarvele ning eelnõu ei ole seotud kohalike omavalitsuse üksuste tegevusega.

8. Rakendusaktid

Eelnõuga ei kehtestata uusi rakendusakte. DORA määruse rakendumisel tuleks korrigeerida asjakohaste Finantsinspektsiooni soovituslike juhendite kohaldamisala, et oleks üheselt selge, et need, kes DORA määruse kohaldamisalasse ei kuulu, siis neile jääb juhend kohalduma.

9. Seaduse jõustumine

Seadus jõustub osaliselt 17. jaanuaril 2025. a. Jõustumise tähtaeg on seotud DORA nõuete rakendamise kuupäevaga, milleks on 17. jaanuar 2025. a. Muudatused, mis ei ole seotud DORA direktiivi ülevõtmisega, jõustuvad üldkorras.

10. Eelnõu kooskõlastamine ja huvirühmade kaasamine

Eelnõu esitatakse läbi eelnõude infosüsteemi EIS kooskõlastamiseks ministeeriumidele ja Finantsinspektsioonile ning arvamuse avaldamiseks Riigikantseleile, Riigi Infosüsteemide Ametile, Eesti Pangale, MTÜ FinanceEstonia-le, Eesti Pangaliidule, Eesti Kindlustusseltside Liidule, Eesti Kindlustusmaaklerite Liidule, Eesti Hoiu-laenuühistute Liidule, Nasdaq Tallinna Börsile, Nasdaq CSD SE Eesti filiaalile, Eesti Kaubandus-Tööstuskojale, Eesti Väike- ja Keskmiste Ettevõtjate Assotsiatsioonile, Eesti Infotehnoloogia ja Telekommunikatsiooni Liidule ja muudele finantssektori ettevõtetele.

Algatab Vabariigi Valitsus
…… 2024
(allkirjastatud digitaalselt)

Heili Tõnisson
Valitsuse nõunik

LISA. Euroopa Liidu direktiivi ja Eesti õigusakti vastavustabel

EL direktiivi (EL) 2022/2556 norm	**Muudetav direktiivi säte**	**EL-i õigusakti normi ülevõtmise kohustus** (Jah, ei, valikuline)	**EL-i õigusakti normi sisuliseks rakendamiseks kehtestatavad riigisisesed õigusaktid**	**Kommentaar**
Art 1 p 1	2009/65/EÜ art 12 lg 1, teine lõik, a	Jah	IFS § 344 lg 3 p 3, § 345 lg 1^1	
Art 1 p 2	2009/65/EÜ art 12 lg 3	Ei	-	Ei ole vaja üle võtta, Komisjoni kohustus
Art 2 p 1	2009/138/EÜ art 41 lg 4	Jah	KindlTS § 96 lg 7^1 ja 105 lg 2 p 2	
Art 2 p 2	2009/138/EÜ art 50 lg 1, a ja b	Ei	-	Ei ole vaja üle võtta, kohaldub Komisjonile
Art 3	2011/61/EL art 18 lg 1	Jah	IFS § 344 lg 3 p 3, § 345 lg 1^1	
Art 3	2011/61/EL art 18 lg 2	Ei	-	Ei ole vaja üle võtta, kohaldub Komisjonile
Art 4 p 1	2013/36/EL art 65 lg 3, a	Jah	KAS § 99 lg 1 p 4^1	
Art 4 p 2	2013/36/EL art 74 lg 1, esimene lõik	Jah	KAS § 82^4 lg 1	
Art 4 p 3	2013/36/EL art 85 lg 2	Jah	KAS § 82^4 lg 2	
Art 4 p 4	2013/36/EL art 97 lg 1, d	Jah	KAS § 96 lg 5	
Art 5 p 1, a	2014/59/EL art 10 lg 7, c	Jah	FELS § 29 lg 1 p 5	
Art 5 p 1, b	2014/59/EL art 10, lg 7, q	Jah	FELS § 29 lg 1 p 8	
Art 5 p 1, c	2014/59/EL art 10 lg 9	Ei	-	EBA kohustus
Art 5 p 2, a	2014/59/EL lisa, A jagu	Jah	FELS § 11 lg 1 p 19	
Art 5 p 2, b	2014/59/EL lisa, B jagu	Jah	FELS § 28 lg 5 p 14^1 ja 14^2	
Art 5 p 3, c	2014/59/EL lisa, C jagu	Jah	FELS § 33 lg 4 p 4 ja 4^1	
Art 6 p 1, a	2014/65/EL art 16 lg 4	Jah	VpTS § 81^1 lg 1^1	
Art 6 p 1, b	2014/65/EL art 16 lg 5	Jah	VpTS § 82^6 lg 4	

Art 6 p 2, a	2014/65/EL art 17 lg 1	Jah	VpTS § 82^{15} lg 1 ja 5	
Art 6 p 2, b	2014/65/EL art 17 lg 7, a	Ei	-	ESMA kohustus
Art 6 p 3, a	2014/65/EL art 47 lg 1, b	Jah	VpTS § 124^{6} lg 1	
Art 6 p 3, b	2014/65/EL art 47 lg 1, c	Jah	VpTS § 124^{6} lg 3	Muudatus näeb ette 2014/65/EL art 47 lg 1 punkti c kustutamise, kuid Eesti õigusesse ülevõtmisel ühtegi sätet kehtetuks ei tunnistata, vaid korrigeeritakse § 124^{6} lg 3 sõnastust.
Art 6 p 4, a	2014/65/EL art 48 lg 1	Jah	VpTS § 125^{1} lg 2	
Art 6 p 4, b	2014/65/EL art 48 lg 6	Jah	VpTS § 125^{2} lg 1	
Art 6 p 4, c	2014/65/EL art 48 lg 12, a ja g	Ei	-	ESMA kohustus
Art 7 p 1	(EL) 2015/2366 art 3, j	Jah	MERAS § 4 lg 1 p 9	
Art 7 p 2, a	(EL) 2015/2366 art 5 lg 1, esimene lõik, e, f ja h	Jah	MERAS § 15 lg 1 p 9, § 50 lg 3 p 9 ja 11	
Art 7 p 2, b	(EL) 2015/2366 art 5 lg 1, kolmas lõik	Jah	MERAS § 15 lg 1^{1} p 2	
Art 7 p 3	(EL) 2015/2366 art 19 lg 6, teine lõik	Jah	MERAS § 62 lg 2	
Art 7 p 4	(EL) 2015/2366 art 95 lg 1	Jah	MERAS § 63^{5} lg 3	
Art 7 p 5	(EL) 2015/2366 art 96 lg 7	Jah	MERAS § 63^{6} lg 5	
Art 7 p 6	(EL) 2015/2366 art 98 lg 5	Ei	-	EBA kohustus
Art 8	(EL) 2016/2341 art 21 lg 5	Jah	IFS § 223 lg 2, § 344 lg 3 p 3, § 345 lg 1^{1}	
Art 9	-	Ei	-	Ei ole vaja üle võtta, direktiivi ülevõtmise säte.
Art 10	-	Ei	-	Jõustumissäte
Art 11	-	Ei		Ei ole vaja üle võtta, direktiivi adressaatide säte.

Määruse (EL) 2022/2554 säte	**EL-i õigusakti normi ülevõtmise kohustus** (Jah, ei, valikuline)	**EL-i õigusakti normi sisuliseks rakendamiseks kehtestatavad riigisisesed õigusaktid**	**Kommentaar**
Art 2 lg 4	Valikuline		Eesti valik on rakendada liikmesriigi valikukohta. Seega art 2 lg 4 nimetatud isikud jäävad DORA kohaldamisalast välja.
Art 19 lg 1	Valikuline	Finantssektori seadustes eraldi sätted intsidentidest teavitamis kohta	Eesti valik on, et finantsasutus teavitab tõsisest intsidendist samaaegselt nii FI-d kui ka NIS2 asutust ehk RIA-t.
Art 26 lg 9	Valikuline		Eesti on otsustanud valikut mitte kasutada.
Art 32 lg 5	Jah	FIS § 46 lg 10	Juhtiva järelevalveasutuse teavitamine, et FI osaleb järelevalvefoorumi töös.
Art 53			Art 53 kohustab liikmesriike teavitavama komisjoni, ESMAt, EBAt ja EIOPAt oma õigus- ja haldusnormidest, millega võetakse üle DORA määruse 7. peatükk, sealhulgas asjaomastest kriminaalõiguse sätetest hiljemalt 17. jaanuariks 2025.
Määruse (EL) 2022/2554 7. peatükk			
Art 46	Otsekohalduv määrus	FIS § 2 lg 1	
Art 47	Otsekohalduv määrus	FIS § 47^{11} lg 1–3	
Art 48	Otsekohalduv määrus	FIS § 6 lg 1 p 6, § 46 lg 1 ja lg 2 p 1–3	
Art 49 lg 1	Ei		ESA-de kohustus
Art 49 lg 2	Otsekohalduv määrus	FIS § 46 lg 1 ja lg 2 p 1–3 § 47^{11} lg 6	
Art 50 lg 1		IFS ptk 30, KAS ptk 9, KindlTS ptk 12, MERAS ptk 12, VpTS ptk 24, EVKS ptk 6	
Art 50 lg 2–6, art 51 ja 54	Otsekohalduv määrus	IFS § 455 lg 3^{2}, § 456 lg 1, § 458,§ 460 ja § 503^{4}, KAS § 99, § 101, § 103, § 103 lg 3^{3}, ja § 134^{26}, KindlTS § 224 lg	

		3, § 227, § 228, § 231 ja § 257^{1}, MERAS § 90 lg 2, § 95, § 97, § 100 ja 109^{1}, VpTS § 230 lg 7, § 230^{3}, § 232, § 234 ja § 237^{90}, EVKS § 39, 39 lg 4^{1}, § 41, § 42 ja § 46^{11} + HMS+ FIS § 5 lg 2 + FIS § 54 lg 3, 5	
Art 52	Valikukoht		Eesti ei ole kasutanud seda võimalust.
Art 55		FIS § 54	
Art 56		FIS § 54^{2} lg 4	