

Finantsinspektsiooni seaduse ja teiste seaduste muutmise seaduse eelnõu¹ 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 sätestatud:

- Euroopa Parlamendi ja nõukogu määruses (EL) 2022/2554², 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) 2022/2556³, 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 tagatakse 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;

¹ Esimesel kooskõlastusel käinud eelnõu nimetus: finantskriisi ennetamise ja lahendamise seaduse ning teiste seaduste muutmise seaduse eelnõu

² <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32022R2554>

³ <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32022L2556>

- kindlustus- ja edasikindlustusandjad;
- kindlustusvahendajad (v.a kuni keskmise suurusega vahendajad);
- krüptovarateenuse osutajad ja varapõhiste tokenite emitendid;
- reitinguagentuurid;
- kriitilise tähtsusega võrdlusaluste haldurid;
- ühisrahastamisteenuse osutajad;
- väärtpaperistamise registrid;
- väärtpaperite 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 osapoolst IKT teenuseosutajad, kelle suhtes kohaldub EL-ülene järelevaldamisraamistik.

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 ettevõtte 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 rakendamiseks seotud sätteid 17. jaanuaril 2025. a. Kindlustusummade tõstmiseks muudatused jõustuvad 9.oktoobril 2024. 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 keeleteimetaja 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 juuliks⁴.

Eelnõuga muudetakse:

- Finantsinspektsiooni seadust (edaspidi *FIS*) redaktsioonis RT I, 06.07.2023, 28;
- finantskriisi ennetamise ja lahendamise seadust (edaspidi *FELS*) redaktsioonis RT I, 17.03.2023, 7;
- investeerimisfondide seadust (edaspidi *IFS*) redaktsioonis RT I, 06.07.2023, 34;
- hoiu-laenuühistute seadust (edaspidi *HLÜS*) redaktsioonis RT I, 05.05.2022, 12;
- kindlustustegevuse seadust (edaspidi *KindlTS*) redaktsioonis RT I, 17.03.2023, 12;
- krediidiandjate- ja -vahendajate seadust (edaspidi *KAVS*) redaktsioonis RT I, 17.03.2023, 13;
- krediidiastutuste seadust (edaspidi *KAS*) redaktsioonis RT I, 17.03.2023, 17;
- makseasutuste ja e-raha asutuste seadust (edaspidi *MERAS*) redaktsioonis RT I, 17.03.2023, 18;
- väärtpaperite registri pidamise seadust (edaspidi *EVKS*) redaktsioonis RT I, 17.03.2023, 11;
- väärtpaperituru seadust (edaspidi *VpTS*) redaktsioonis RT I, 06.07.2023, 128.

Eelnõu on seotud järgmiste EL õigusaktidega:

- DORA määrus;
- DORA direktiiv;
- Komisjoni delegeeritud määrus (EL) 2024/896⁵, millega muudetakse Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/97 selliste regulatiivsete tehniliste standardite osas, millega kohandatakse kindlustus-, edasikindlustus- ja kõrvaltegevusena pakutava kindlustuse vahendajate ametialase vastutuskindlustuse ning finantssuutlikkuse baassummasid eurodes (edaspidi *kindlustussummade muutmise määrus*).

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 (edaspidi *HOS eelnõu*)⁶. NIS2 direktiivi ülevõtmiseks on MKM koostamas küberturvalisuse seaduse muutmise seaduse eelnõu.

⁴ VVTP-s on viide direktiivile (EL) 2022/1556, õige on (EL) 2022/2556.

⁵ Delegeeritud määrus - EL - 2024/896 - EN - EUR-Lex (europa.eu)

⁶ <https://eelnoud.valitsus.ee/main/mount/docList/ad7af8cd-617c-45f3-b850-78ad002f6a3a>

Käesoleva eelnõu vastuvõtmiseks on vajalik Riigikogu poolthääle enamuse saamine.

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.

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/EÜ⁷, 2009/138/EÜ⁸, 2011/61/EL⁹, 2013/36/EL¹⁰, 2014/59/EL¹¹, 2014/65/EL¹², (EL) 2015/2366¹³ ja (EL) 2016/2341¹⁴, on need nõuded väga erinevad ja kohati mittetäielikud. Kuigi viidatud liidu õigusaktides on käsitletud operatsiooniriski norme põhjalikumalt, on keskendunud sageli traditsioonilisele kvantitatiivsele riski käsitlevale lähenemisviisile (kehtestades riski hõlmamiseks kapitalinõuded), mitte sihipärasele 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 pressiteates¹⁵ 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 väikepankad 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 talitluspiidavusega seotud riskid keskmisest kõrgemad. Lisaks teatasid mitmed tarkvaratootjad

⁷ Euroopa Parlamendi ja nõukogu direktiiv 2009/65/EÜ, 13. juuli 2009, vabalt võõrandatavatesse väärtpaberitesse ühiseks investeerimiseks loodud ettevõtjaid (eurofondid) käsitlevate õigus- ja haldusnormide kooskõlastamise kohta EMPs kohaldatav tekst

⁸ Euroopa Parlamendi ja Nõukogu direktiiv 2009/138/EÜ, 25. november 2009, kindlustus- ja edasikindlustustegevuse alustamise ja jätkamise kohta (Solventsus II) EMPs kohaldatav tekst

⁹ 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

¹⁰ Euroopa Parlamendi ja nõukogu direktiiv 2013/36/EL, 26. juuni 2013, mis käsitleb krediitiasutuste tegevuse alustamise tingimusi ning krediitiasutuste 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

¹¹ Euroopa Parlamendi ja nõukogu direktiiv 2014/59/EL, 15. mai 2014, millega luuakse krediitiasutuste 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

¹² 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

¹³ 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)

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

¹⁵ <https://fi.ee/et/uudised/finantsinspektsioon-suunab-panku-maandama-it-riske>

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 aruandes¹⁶, 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 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 raportis¹⁷ 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 äriefunktsioonid, 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 korruga 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

¹⁶ https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

¹⁷ <https://www.esrb.europa.eu/pub/pdf/reports/esrb.macropprudentialtoolscyberresilience220214~984a5ab3a7.en.pdf?888a06fcb36d2c1ce41594efd67a4c88>

	varunduspõhimõtted ja -menetlused, ennistamise ja taastamise menetlused ja meetodid, tagamaks IKT-süsteemide ja andmete ennistamine minimaalse seisuaaja, 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 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:	<ul style="list-style-type: none"> - 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:	<ul style="list-style-type: none"> - teavitada finantsasutust, et ta on teate kätte saanud. - teavitada intsidendist Euroopa Järelevalveasutusi (ESA-sid), Euroopa Keskpanga (EKP) (asjakohasel juhul), riiklikke pädevaid asutusi, CSIRTi, kriisilahendusasutusi ja muid asutusi vastavalt riigisisesele õigusele.
FI võib:	<ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - hinnata valmisolekut intsidentide käsitlemiseks; - tuvastada nõrgad kohad ja puudused süsteemides ja inimressuris; - rakendada vajadusel parendusmeetmeid.
Kuidas testitakse?	Finantsasutus peab läbi viima järgmised testimised: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - ohuteabel põhinev läbistustestimine (küberrünnete matkimine); - iga 3a tagant (pädev asutus võib sagedust muuta); - pädev asutus määrab testimises osalevad finantsasutused (väljastatud mikroettevõtjad ja need, kes kuuluvad leebema IKT riskijuhtimise režiimi alla); - testimine toimub <i>live</i> keskkonnas; - lubatud nii välised testijad kui ka teatud tingimustel sisetestijad; - testis osalevad ka kolmandast isikust IKT teenuseosutajad; - <i>Single public authority</i> (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 funktsioone;
- 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 teenuseosutaja 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.

Järelevaatamisfoorum (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 kontrole (moodustatakse <i>joint examination team</i>).
	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).
-----------------------------	---

	<ul style="list-style-type: none"> - 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.	<ul style="list-style-type: none"> - 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 mõjuanalüüsi¹⁸: „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 kohaselt¹⁹, 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 finantsüsteemi, 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 teabevoold peaksid

¹⁸ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0198>

¹⁹ NIS2 direktiiv

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 kohta²⁰, sealhulgas finantsteenuste digitaalse tegevuskerksuse 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 teavituse vormi (sama teavituse normi 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 läbistustestimisega. 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 krediidasutuste puhul on pädevaks asutuseks Euroopa Keskpank, kelle järelevalve alla kuulub 1. märtsi 2023. a seisuga 110 institutsiooni, neist 4 Eesti krediidasutust ning süvatestimise kohustus on eelkõige olulistel

²⁰ <https://eelnoud.valitsus.ee/main/mount/docList/c969654c-9691-4b71-abb1-7baa3e665d13>

krediidiasutustel²¹, 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.

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. Konsulterides 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. Siiski on ka NIS2 direktiivi artikli 2 lõikes 10 sätestatud, et käesolevat direktiivi ei kohaldata üksuste suhtes, mille liikmesriigid on kooskõlas määruse (EL) 2022/2554 artikli 2 lõikega 4 kõnealuse määruse kohaldamisalast välja jätnud.

Kuna hoiu-laenuühistute seaduseelnõu²² menetlus on veel pooleli, siis hetkel on võetud lähenemine, et hoiu-laenuühistutele ei kohaldata DORA nõudeid. Oluline on siinjuures tähelepanu juhtida asjaolule, kui hoiu-laenuühistust peaks saama ühistupank, siis kohalduvad talle viidatud seaduseelnõu kohaselt KAS nõuded, mis hõlmavad endas ka kohustust rakendada DORA määruses sätestatud nõuded.

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.

²¹ See veel selgub, millised finantsasutused peavad süvatestimisi läbi viima, kuid eelduslikult on nendeks näiteks olulised pangad ja börs.

²² <https://eelvoud.valitsus.ee/main/mount/docList/db5ae432-6d08-4896-972c-101c32e9d2ce>

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 liikmesriigi valikukohaga, kuid huvirühmadega konsultatsiooni käigus tõstatus teema, milline asutus on pädev asutus DORA määruses sätestatud ülesannete täitmisel ja järelevalve teostamisel.

DORA järelevalvet on määratud teostama finantsjärelevalve asutus

- DORA pädev asutus on määratletud DORA määruse artiklis 46;
- tegemist on sama asutusega, kes teostab finantsjärelevalvet finantsasutuse üle;
- DORA määruse artiklis 46 on viited finantssektori EL direktiividele ja määrustele, mis reguleerivad finantsasutuste tegevust ja järelevalvet. Liikmesriik on pidanud määrama pädeva asutuse, kes teostab EL finantssektori direktiivides ja määrustes sätestatud nõuete täitmise üle järelevalvet;
- Eestis teostab artiklis 46 viidatud EL direktiivides ja määrustest sätestatud nõuete täitmise üle järelevalvet FI. Oluliste krediidasutuste puhul on pädevaks asutuseks Euroopa Keskpank;
- selleks, et muu asutuse (nt RIA) saaks määrata DORA pädevaks asutuseks, tuleks Eestis finantsjärelevalve korraldus ümber teha.

Eesti finantsjärelevalve korraldust ei ole käesoleva eelnõu raames muudetud

- Eestis on finantssektori järelevalvealane kompetents antud täies mahus FI-le;
- DORA määruse väljatöötamisel liidus otsustati määrata pädevaks asutuseks sama asutus, kes vastutab finantsjärelevalve eest finantssektoris, tagades sedasi, et finantsjärelevalve asutusel on tervikpilt kõikidest finantssektori riskidest, sh IKT-riskidest;
- IKT-riskide juhtimine on osa finantsasutuse riskijuhtimissüsteemist. Riskipõhiste kapitalinõuete puhul ka osa kapitalijuhtimisest, mistõttu ei saa finantsasutuse küberriske vaadelda eraldiseisvalt, vaid see moodustab koos teiste riskide ja finantsasutuse tegevusvaldkondadega terviku;
- IKT- riskide järelevalve on oluline osa finantsasutuse operatsiooniriskide järelevalvest;
- IKT-teenuste edasiandmine on osa finantsasutuse teenuste ja tegevuste edasiandmise raamistikust;
- finantssektor on terviklik, mida tuleb vaadelda kompaktselt ning järelevalve pädevuse jagamisega teatud valdkondades ei ole võimalik tagada finantssektori järjepidevust, stabiilsust ja usaldusväarsust;
- IKT-d ja selle raames küberturvalisuse põhimõtete rakendamist tuleb vaadelda kui tehnilist lahendust ja üht valdkonda mitmekülgsest finantssektorist;
- FI-l on olemas finantssektori eripärade tundmine ja vajalike järelevalveliste meetmete rakendamisel parim teadmine, sealhulgas teadmised, millised on konkreetse subjekti puhul just need asjakohased meetmed, mis on piisavad ühelt poolt rikkumiste kõrvaldamiseks, kuid teiselt poolt ei seaks rakendatavad meetmed ohtu finantssektori korrapärasest toimimisest ja klientide huve;
- FIS § 3 kohaselt teostab Finantsinspeksioon riiklikku finantsjärelevalvet finantssektori stabiilsuse, usaldusväarsuse 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;

- määrates muu asutuse finantsjärelevalve pädevaks asutuseks, ei pruugi sellel asutusel olla teadmisi finantssektori eripäradest ning tõhusatest, efektiivsetest ja tulemuslikuks järelevalve teostamiseks vajalikest mitmetahulistest ja terviklikest protsessidest.

Näide järelevalve terviklikkuse kohta:

- **näide 1.** Krediidiasutuste tegevus on reguleeritud direktiivis 2013/36/EL. Direktiivi artikli 74 lõike 1 kohaselt: „Finantsinstitutsioonidel peab olema kindel äriühingu juhtimise korraldus, mis hõlmab selget organisatsioonilist ülesehitust, mille puhul vastutusosalad on selgesti määratletud, läbipaistvad ja järjepidevad, tõhusaid protseduure riskide või võimalike riskide kindlaksmääramiseks, juhtimiseks, jälgimiseks ja nendest teatamiseks, piisavat sisekontrollikorda, sealhulgas usaldusväärne juhtimis- ja raamatupidamiskord, võrgu- ja infosüsteeme, mis on loodud ja mida hallatakse kooskõlas määrusega (EL) 2022/2554, ning tasustamispoliitikat ja -tavasid, mis on kooskõlas usaldusväärse ja tõhusa riskijuhtimisega ja edendavad seda.“
- **näide 2.** Direktiivi 2014/65/EL artikli 16 lõike 4 kohaselt: „ Investeerimisühing võtab mõistlikke meetmeid, et tagada investeerimisteenuste osutamise ning investeerimistegevuse järjepidevus ja korrapärasus. Selleks kasutab investeerimisühing sobivaid ja proportsionaalseid süsteeme, sealhulgas info- ja kommunikatsioonitehnoloogia (IKT) süsteeme, mis on loodud ja mida hallatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2022/2554 artikli 7 kohaselt, samuti sobivaid ja proportsionaalseid ressursse ja protseduure.“
- **näide 3.** Makseasutuste direktiivi artikli 19 lõike 6 kohaselt ei või oluliste tööülesannete, sealhulgas IKT-süsteemide edasiandmine toimuda viisil, mis kahjustab oluliselt makseasutuse sisekontrolli kvaliteeti ja pädevate asutuste võimet kontrollida ja jälgida, et makseasutused täidavad kõiki selles direktiivis sätestatud kohustusi.
- **näide 4.** Kindlustusdirektiivi 2009/138/EÜ artikli 41 kohaselt võtavad kindlustus- ja edasikindlustusandjad vajalikud meetmed, et tagada oma ülesannete täitmisel, sealhulgas eriolukordi käsitlevate plaanide väljatöötamisel, järjepidevus ja korrapärasus. Kindlustus- ja edasikindlustusandjad kasutavad selleks asjakohaseid ja proportsionaalseid süsteeme, ressursse ja menetlusi ning loovad eelkõige võrgu- ja infosüsteemid ja haldavad neid kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) 2022/2554
- näidete kohaselt ei ole FI-l võimalik teostada krediidiasutuse juhtimise korralduse, investeerimisühingu ja kindlustusandja süsteemide ning makseasutuse tegevuste edasiandmise nõuete üle terviklikku järelevalvet, jättes järelevalvest välja võrgu- ja infosüsteemide järelevalve.
- analoogsed näited on finantssektori EL õigusaktides veel.

Finantssektori IKT-riskide järelevalve seni:

- nagu eespool osutatud, on IKT riskid osa finantssektori riskijuhtimisest ning FI on IKT-riskide alast järelevalvet teostanud aastataid;
- finantsasutused on pidanud aastaid järgima FI kehtestatud nõudeid finantsjärelevalve subjekti infotehnoloogia ja infoturbe korraldusele²³, nõudeid finantsjärelevalve subjekti talitluspidevuse korraldusele, EBA suuniseid IKT- ja turvariskide juhtimiseks²⁴ ning

²³ https://www.fi.ee/sites/default/files/2020-06/N%C3%B5uded%20finantsj%C3%A4relevalve%20subjekti%20infotehnoloogia%20ja%20infoturbe%20korraldusele_%20kinnitatud.pdf

²⁴ https://fi.ee/sites/default/files/2020-03/pp%20nr%2008%20Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management_COR_ET.pdf

- EIOPA info- ja kommunikatsioonitehnoloogia turbe- ja juhtimissuuniseid²⁵ ja pilveteenuse osutajatele tegevuse edasiandmise suunised²⁶. Nõuete täitmise üle teostab järelevalvet FI;
- DORA on suures ulatuses koostatud viidatud EBA ja EIOPA suuniste baasilt ning FI-l on praktika ja protsessid loodud vastava järelevalve teostamiseks;
 - seega ei ole IKT-riskide järelevalve ja DORA määrusest tulenevad nõuded FI jaoks midagi uut;
 - FI järelevalveprotsesside ja -vahendite hulka kuuluvad mh SREP²⁷ hinnangud, erinevad analüüsid, kohapealsete kontrollide läbiviimine, koostöö Euroopa järelevalveasutustega ja vastavates töögruppides osalemine ning teabe ja praktika jagamine jne;
 - FI enda hinnangul võib senist järelevalvet hinnata edukaks, kuna antud perioodil puuduvad täielikult olulise mõjuga suuremad intsidendid, mis oleks tulenenud küberriski realiseerumisest finantssektoris;
 - FI on alustanud DORA määruse rakendamiseks vajalike esmaste tegevuste ja protsessidega, et DORA määruse nõudeid veelgi edukamalt rakendada.

Puudub mõjuanalüüs finantsjärelevalve korralduse ümber tegemise kohta

- finantssektor järelevalves ümberkorralduste tegemine eeldab põhjalikku mõjuanalüüsi, sealhulgas seoses mõjuga riigieelarvele;
- RIA-le finantsjärelevalves osalise pädevuse andmine omab olulist mõju riigieelarvele (riigieelarve suurendamine), kuna tuleb arvestada täiendavate kuludega (RIA järelevalve alla kuuluks ligemale 100 finantsasutust, sh krüptovaratteenuse osutajad);
- RIA hakkaks kuuluma Euroopa järelevalvesüsteemi²⁸, olles pädev asutus EBA, EIOPA ja ESMA määruste tähenduses²⁹ ja kohustudes järgima viidatud määrustes pädevatele asutustele kohalduvaid nõudeid, sealjuures täitma EBA, EIOPA ja ESMA suuniseid ja soovitusi, esitama EBA-le, EIOPA-le ja ESMA-le regulaarselt teavet nende ülesannete täitmiseks ning osalema EBA, EIOPA ja ESMA töögruppides;
- seega, lisaks kulude suurenemisega seoses DORA nõuete järelevalvega, kaasnevad täiendavad kulud seoses kuulumisega Euroopa järelevalvesüsteemi. EBA, EIOPA ja ESMA eelarve moodustub osaliselt pädevate asutuste osamaksetest;
- samuti moodustatakse DORA alusel tekkiva kriitilise tähtsusega kolmandast osapoolst IKT teenuseosutajate liiduülese järelevalve kohustuse täitmiseks vastav järelevalve just finantssektori järelevalveasutuste ressurssidest;
- kui jätkata olemasolevat finantsjärelevalve poliitikat, kus finantssektori järelevalve teostamine on vaid FI pädevuses, mõju riigieelarvele puudub;
- Eestis kehtiva finantssektori rahastusmudeli puhul maksavad järelevalvesubjektid järelevalvetasu FI-le ja seeläbi finantseerivad järelevalve teostamist;
- finantssektori järelevalvekorralduse ümber tegemise korral tuleks riigieelarvet kasutada ka finantsjärelevalve eesmärkide realiseerimiseks. Viimaste tarbeks ongi loodud eelnevalt kirjeldatud rahastusmudel, mis ei sõltu riigieelarve vahenditest.

Teised riigid

- teadaolevalt ka teiste Euroopa riikide (nt Läti, Leedu ja Soome) korral DORA pädevaks asutuseks just finantsjärelevalve asutus;

²⁵ <https://fi.ee/sites/default/files/2021-06/pp%20nr%2006%20eiopa-gls-ict-security-and-governance-et.pdf>

²⁶ <https://fi.ee/sites/default/files/2020-06/pp%20nr%2003%20Guidelines%20on%20outsourcing%20to%20cloud%20service%20providers%20-%20ET.pdf>

²⁷ Supervisory review

²⁸ <https://www.europarl.europa.eu/factsheets/et/sheet/84/euroopa-finantsjarelevalve-susteen>

²⁹ EBA määruse näitel on pädevad asutused määratletud artikli 4 punktis 2 ehk kui määrata näiteks RIA määruse (EL) nr 575/2013 artikli 4 lõike 1 punkti 40 kohaselt kaas pädevaks asutuseks, oleks RIA pädev asutus ka EBA määruse tähenduses. Sama on EIOPA ja ESMA määrustega.

- kogu Euroopa mudel on üles ehitatud selliselt, et pädev asutus on finantsjärelevalveasutus ning hetkel ei ole teada ühtegi näidet, kus sedalaadi pädevus viiakse ära finantsjärelevalve asutusest;
- finantsjärelevalveasutusi koondavad töögrupid, erinevad (kriisi)harjutused jne lähtuvad just sellest põhimõttest, et finantssektori pädev järelevalveasutus on pädevaks asutuseks ka DORA määruse alusel.

Koostöö

- 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 § 47¹¹ juures), mis annab võimaluse kaasata DORA nõuete järelevalvesse ka RIA, nähes muu hulgas ette teabe vahetamise õigused;
- teavitused tõsistest IKT-intsidentidest edastatakse mh RIA-le (vt valikukoht 1) ning DORA ei piira RIA võimalusi abistada finantsasutusi, sealjuures on DORA määruse artikli 22 lõike 1 sissejuhatavas osas selge viide, et NIS2 pädeva asutus saab vastavalt liikmesriigi õigusele pakkuda finantsasutusele tehnilist panust, nõuandeid või parandusmeetmeid ning järeelmeetmeid;
- seega on RIA kaasatud oma küberturbe pädevusega finantssektori järelevalvesse.

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 ³⁰ 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. - 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 ³¹ ja keskmise suurusega ³² kindlustusvahendajatele.
Kindlustusagendid, kellele hakkab DORA kohalduma (sulgudes agente kokku)	0 (378)	- DORA määruse ei kohaldu mikrodele, väikestele ja keskmise suurusega kindlustusvahendajatele.
Fondivalitsejad	12	- mikrodele leevendused ptk-des 2, 4 ja 5. - kohustusliku ja täiendava pensionifondi valitsejatele DORA ei kohaldu.

³⁰ kus töötab vähem kui 10 inimest ning kelle aastakäive ja/või aastabilansi kogumaht ei ületa 2 miljonit eurot

³¹ 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

³² 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

Tegevusloaga väikefondi valitsejad	(6)	- DORA määrus neile ei kohaldu.
Registreeritavad väikefondi valitsejad	(75)	- DORA määrus neile ei kohaldu.
Investeeringisühingud	9	- mikrodele leevendused ptk-des 2, 4 ja 5. - leebem IKT-riskijuhtimise režiim (ptk 2) väikestele ja mitteseotud investeeringisühingutele.
Reguleeritud turu korraldaja	1	- mikrodele leevendused ei kohaldu.
Väärtpaberiarveldussüsteemi korraldaja	1	- mikrodele leevendused ei kohaldu.
Väärtpaberiturukauplemiskohad	1	- mikrodele leevendused ei kohaldu.
Keskne vastaspool	0	- mikrodele leevendused ei kohaldu.
Aruandlusteenuse osutaja	0	- mikrodele leevendused ptk-des 2, 4 ja 5.
Ühisrahasusteenuse osutajad	2	- mikrodele leevendused ptk-des 2, 4 ja 5.
Hoiu-laenuühistud	(17) ³³	- 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 ³⁴	- mikrodele leevendused ptk-des 2, 4 ja 5.
Varapõhiste tokenite emitendid (MICAR tegevusloaga)	0	- mikrodele leevendused ptk-des 2, 4 ja 5.

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

³³ <https://statistika.eestipank.ee/failid/mbo/hly.html>

³⁴ Käesoleval hetkel ei ole veel võimalik MICAR alusel tegevusloba taotleda. 2024. aasta aprilli seisuga on RahaPST alusel tegutsemas 49 virtuaalvääringuteenuse pakkujat.

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

NIS2 direktiivi kohaldatakse direktiivi I või II lisa osutatud sellist liiki avalik-õiguslike või eraõiguslike üksuste suhtes, mis kvalifitseeruvad soovitusel 2003/361/EÜ³⁵ 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. Siiski peaksid liikmesriigid jätkuvalt kaasama finantssektori oma küberturvalisuse strateegiasse. DORA määruse kohaldamisalasse kuuluvate üksuste suhtes tuleks ka edaspidi kohaldada sätteid, mis käsitlevad küberkriiside ohjamise raamistikke (NIS2 direktiivi artikkel 9) ja EU - CyCLONe'i (NIS2 direktiivi artikkel 16)³⁶. Kuivõrd on oluline, et NIS2 direktiivi alusel säiliks tugevad suhted ja teabevahetus finantssektoriga, võivad Euroopa järelevalveasutused ja DORA määruse alusel pädevad asutused taotleda osalemist koostöörühma tegevuses ning vahetada teavet ja teha koostööd ühtsete kontaktpunktidega, aga ka CSIRTidega ja NIS2 direktiivi kohaste pädevate asutustega. NIS2 direktiivi artikli 24 lõike 1 teise lause kohaselt peaksid liikmesriigid ergutama elutähtsaid ja olulisi üksusi kasutama kvalifitseeritud usaldusteenuseid.

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 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. Lisaks on artikli 8 teises lauses sätestatud, et liikmesriigid võivad vastu võtta või säilitada liikmesriigi õigusnormid, millega saavutada kõnealuste elutähtsa teenuse osutajate toimepidevuse kõrgem tase, tingimusel et need õigusnormid on kooskõlas kohaldatavate liidu õigusnormidega (vt HOS eelnõu ja seletuskirja).

³⁵ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32003H0361>

³⁶ Vt ka [https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52023XC0918\(01\)](https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52023XC0918(01))

Koostöö ja küberturvalisuse strateegia

DORA määrus võimaldab Euroopa järelevalveasutustel ja finantsjärelevalve pädevatel asutustel osaleda koostöörühma tegevuses ning vahetada teavet ja teha koostööd ühtsete kontaktpunktide³⁷, 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)
Krediidasutused ja finantsturutaristud	Kohaldub täies ulatuses.	Kohaldub CER direktiivi II peatükk; Ei kohaldata CER direktiivi art 11 ning III, IV ja VI peatükki. Liikmesriigid võivad vastu võtta või säilitada liikmesriigi õigusnormid, millega saavutada kõnealuste elutähtsa teenuse osutajate toimepidevuse kõrgem tase.	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 krediidasutuse ja finantsturutaristu järelevalvega	FI; EKP (olulised krediidasutused).	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. FI teavitab tõsistest intsidentidest RIA-t ja asjakohasel juhul muid avaliku sektori asutusi.	Koostöö NIS2 päeva asustusega. Kuna DORA pädev on teatud juhtudel ka CER pädev asutus, siis peab tegema koostööd ka teis(t)e CER pädeva(te) asutus(te)ga.	Art 13 – RIA koostöö, sh teabe vahetamine DORA (FI/EKP) ja CER pädevate asutustega ja muude artiklis loetletud asutustega.

³⁷ Iga liikmesriik määrab küberturvalisuse pädevate asutuste seast ühe kontaktpunkti, mis täidab sidepidamisfunktsiooni, et tagada oma liikmesriigi ametiasutuste piirilene koostöö teiste liikmesriikide asjaomaste asutustega ning asjakohasel juhul komisjoni ja ENISAg ning ka valdkondadevaheline koostöö oma liikmesriigi teiste pädevate asutustega.

	FI/EKP saab vajadusel konsulteerida RIA ja muu liikmesriigi NIS2 pädeva asutusega.		
--	--	--	--

2.6. Eelnõu kooskõla EV põhiseadusega (PS)

2.6.1. Eelnõuga riivatakse ettevõtlusvabadust (PS § 31), kuna seadusega kehtestatakse nõuded finantsasutuste digitaalsele tegevuskerksusele. Ettevõtlusvabadus annab isikule õiguse nõuda, et avalik võim ei sekkuks tema ettevõtlusena käsitatavasse tegevusse. Ettevõtlusvabadust võib piirata seadusega. Finantsasutustele on nende tegevuse iseloomust tulenevalt avalikkusel kõrgemad ootused ja nõuded, seetõttu on nendele kehtestatud ulatuslikult regulatsioone nii EL tasandil kui siseriiklikult. Antud juhul peavad ettevõtjad digitaalse tegevuskerksuse nõuete rakendamiseks teatud ümberkorraldusi tegema, nt juhtimisstruktuuri tõhustamine. Samuti peavad nad EL ja seaduse nõuetega kooskõlla viima IKT riskide juhtimise nõuded, sh nõuded küberturvalisuse tagamiseks. Siiski ei ole see esimene kord, kui finantsasutusele sarnaseid nõudeid esitatakse, sellele vaatamata piirab see ettevõtja tegevust ning eeldab omakorda ettevõtjalt täiendavate rahaliste kulutuste tegemist.

Eelnõuga ette nähtud piirangud on mõistlikud. Kuigi digitaalse tegevuskerksuse nõuded on ühest küljest finantsasutusi koormavad, siis teisest küljest tagab see nende tegevuse toimimise ja jätkusuutlikkuse igapäevases majanduses üleüldiselt. See omakorda on seotud avaliku huviga, kuna finantsasutuste stabiilsus aitab kaasa ka riigi majanduse toimimise stabiilsusele. Lisaks aitab nõuete rakendamine ära hoida kahjusid, mis võiks kaasneda IKT-riskidega, mis kaasnevad finantsüsteemi küberohtudega ning IKT-katkestustega. IKT kasutamine on finantsteenuste osutamisel omandanud keskse rolli, kusjuures see on igapäevaste funktsioonide toimimise jaoks kriitilise tähtsusega. Finantssektori digitaliseerimine on süvendanud seoseid ja sõltuvust nii finantssektori sees kui ka finantssektori ja kolmandate isikute taristu ja kolmandast isikust teenuseosutajate vahel. See kõik toob kaasa küberintsidentide riski, mis ei ole ainult Eesti kohalik probleem. Nende riskide maandamiseks on oluline kehtestada ja järgida digitaalse tegevuskerksuse nõudeid.

Lisaks kaitsevad eelnõuga kehtestatavad finantsasutuste digitaalse tegevuskerksuse nõuded isikute omandit, kes on oma raha usaldanud finantsasutuste hoolde. PS § 32 kohaselt on igäihe omand puutumatu ja võrdselt kaitstud. Antud eelnõuga võtab riik meetmeid, et see isikute õigus saaks tagatud.

Seega on digitaalse tegevuskerksuse nõuete kehtestamine finantsasutustele põhjendatud ja proportsionaalne.

2.6.2. Eelnõuga kehtestatakse väärteokaristused DORA määruses sätestatud digitaalse tegevuskerksuse nõuete rikkumise eest. Sellega on puutumuses PS § 11, mille kohaselt võib õigusi ja vabadusi piirata ainult kooskõlas seadusega. Samuti riivatakse PS § 31, mille korral mõned ettevõtlusega seotud teod võivad olla kvalifitseeritud väärtegudeks ning nende eest nähakse ette karistused³⁸. Need piirangud peavad olema demokraatlikus ühiskonnas vajalikud ega tohi moonutada piiratavate õiguste ja vabaduste olemust. Karistused on piirangud ning need

³⁸ O. Kask, S. Ehrlich, A. Henberg. PS § 31 kommentaarid, p 33. – Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne, viies, parandatud ja täiendatud väljaanne. Justiitsministeerium: 2020. <https://pohiseadus.ee/sisu/3502>

piirangud olema proportsionaalsed ning ei või olla ülemäärased. Finantssektoris võib IKT-riski realiseerumine mõjutada finantsstabiilsust ja finantssüsteemi usaldusväarsust, seetõttu on vaja ette näha proportsionaalne karistuste rakendamise kord. Lisaks kaasneb eelnõu kohaselt karistuse määramisega ka selle avalikustamine.

Eelnõuga ette nähtavad rahatrahvid on:

1) IFS § 503⁴ ja KAS § 134²⁶, MERAS § 109¹, VpTS § 262³ - rahatrahv 5 000 000 eurot või kuni kahekordse väärteto tulemusel teenitud kasule või ära hoitud kahjule vastavas summas ning juriidilise isiku puhul sama suur trahv, kuid alternatiiviks on kuni kahekordse väärteto tulemusel teenitud kasule või ära hoitud kahjule vastavas summas või kuni 10% juriidilise isiku või tema konsolideerimisgrupi konsolideeritud käibest;

2) KindlTS § 257¹ - rahatrahv 700 000 eurot või kuni kahekordse väärteto tulemusel teenitud kasule või ära hoitud kahjule vastavas summas ning juriidilise isiku puhul 5 000 000 eurot või kuni kahekordse väärteto tulemusel teenitud kasule või ära hoitud kahjule vastavas summas või kuni 10% juriidilise isiku või tema konsolideerimisgrupi konsolideeritud käibest.

Määrad on kooskõlas vastavates seadustes sätestatud määradega. Täpsemad selgitused on toodud vastavate sätete selgituste juures.

Finantsasutuste puhul on väärtetokaristustena ette nähtud rahatrahvid kõrgemas suurusjärgus, kui teistes eluvaldkondades, sest finantssektor põhineb usaldusel. Seadusega pandud kohustuste mitte järgimine võib kaasa tuua ulatuslikud tagajärjed mitte ainult sellele finantsasutusele endale, vaid kogu ühiskonnale. Tänapäeva ühiskonna heaolu sõltub olulisel määral finantssektoris tegutsevate ettevõtjate pakutavatest teenustest ja finantsturgude usaldusväarsusest. Finantssektor on valdkond, mille suhtes valitseb kõrgendatud avalik huvi. Seetõttu peavad sellised karistused olema tulemuslikud, proportsionaalsed ja hoiatavad.

Tavakliendil puuduvad üldjuhul teadmised ja piisav informatsioon finantsteenustega seonduvate riskide hindamiseks ja kehtestatud regulatsioonid peavad looma usaldusväärse keskkonna ning tagama klientide kaitse. Eelnimetatud kohustused võtab iga finantssektori ettevõtja endale turule sisenedes, kusjuures suures osas on regulatsiooni nõuded ka tegevusloa kontrolliesemeks.

Antud juhul on rahatrahv vajalik kuna:

1) sellel on üldpreventiivne positiivne eesmärk. Õiguskord annab avalikkusele selge märgi õigusrikkumise hukkamõistetavuse kohta. Üksnes sunniraha meede ei heidutaks finantsjärelevalvesubjekte nõudeid rikkumast, teades, et nõuete rikkumisele võib järgneda vaid ettekirjutus, s.t ettekirjutuse täitmisel ei ole neil vaja karta rahalist karistust;

2) finantssektori puhul võib iga nõude rikkumisega kaasneda oluline kahju avalikkusele, eelkõige investoritele ja võlausaldajatele, aga ka kolmandatele isikutele. Ettekirjutuse ja sunnirahaga on võimalik nõuda seaduskuulekat käitumist ja kõrvaldada eelkõige selliseid rikkumisi, mille tagajärjed ei avalda mõju kolmandatele isikutele, kuid välistatud ei ole, et mõni, olemuselt kõrvaldatav, seaduse nõuete rikkumine toob kaasa piisava ohu või kahju, et vajalik on ka väärtetokoosseisu sätestamine.

Kokkuvõtvalt, eespool toodud arvesse võttes, on Rahandusministeeriumi hinnangul eelnõuga lisatavad väärtetokoosseisud finantssektori järelevalve seisukohalt olulise tähtsusega ja proportsionaalsed.

3. Eelnõu sisu ja võrdlev analüüs

3.1. Eelnõu § 1. Finantsinspektsiooni seaduse muutmise

FIS § 6 lõike 1 uus punkt 7⁵. 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 § 47¹¹ 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 järelele vaatamise foorumisse. Sellest tuleb ka juhtivat järelele vaatasutust teavitada.

Nimelt reguleerib DORA määrus mh järelele vaatamist kriitilise tähtsusega kolmandast isikust IKT-teenuseosutajate üle. Järelele vaatamise foorum hindab igal aastal ühiselt kõigi kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate järelele vaatamise tulemusi ja leide ning edendab koordineerimismeetmeid, et suurendada finantsasutuste digitaalset tegevuskerksust, edendada IKT kontsentratsiooniriski käsitlemise parimaid tavasid ja uurida riskide valdkonnaülest üle kandumist 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 muutmise (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 § 47¹¹ 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 järelele vaatamise 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 krediitiasutuse 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 -intsidende ning muid kui küberriske, -ohte ja -intsidende, sealhulgas seoses asjakohaste meetmetega, mille on võtnud NIS2 kohased pädevad asutused. Täpsemalt on teabevahetuse ulatus ette nähtud HOS eelnõus (seaduse täiendamine §-ga 41⁵⁶), mille kohaselt Finantsinspeksioon ja Riigi Infosüsteemi Amet vahetavad vastastikku teavet HOS §-s 36 lõikes 3 nimetatud elutähtsaid teenuseid osutavate elutähtsa teenuse osutajate toimepidevuse, neid mõjutavate ohtude, riskide, toimepidevuse tagamiseks rakendatud meetmete ja toimunud sündmuste kohta, samuti asjaomast teavet, mis on vajalik järelevalvemenetluse läbiviimiseks arvestades eriseadusest tulevate piirangutega.

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.

Lõige 3. Selleks, et mitte kohaldada teatud finantsasutustele topelt intsidentidest teavitamise nõudeid, nähakse käesoleva eelnõuga ette järgmine lahendus:

- kui finantsasutuse puhul on mh tegemist elutähtsa teenuse osutajaga hädaolukorra seaduse § 38 lõike 1 tähenduses, siis kohaldub talle DORA määruses ja käesolevas eelnõus sätestatud kohustus teavitada tõsisest IKT intsidendist nii FI-d kui ka RIA-t,
- sellisel juhul ei pea ta topelt teavitama elutähtsa teenuse toimepidevust korraldavat asutust (Eesti Panka) elutähtsa teenuse katkestusest, katkestuse ohust, elutähtsa teenuse toimepidevust oluliselt häirivast sündmusest või sellise sündmuse toimumise vahetust ohust, nagu on sätestatud hädaolukorra seaduses. Oluline on rõhutada, et nii on vaid juhul, kui tegemist on tõsise IKT intsidendiga.
- FI edastab viivitamata nii esialgse teate, vaheraporti kui ka lõppraporti Eesti Pangale.
- krediitiasutuste puhul on lisatud eelnõusse täpsustus (KAS § 92³ lg 2), et DORA kohase teavitusega loetakse hädaolukorra seaduse § 38 lõike 3 punktis 4 sätestatud elutähtsa teenuse osutaja teavitamise kohustus täidetuks.
- juhul, kui tegemist ei ole tõsise IKT intsidendiga DORA tähenduses, kohalduv teavitamisele hädaolukorra seadus ning elutähtsa teenuse osutaja teavitab otse Eesti Panka.

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). Seega, kuna CER direktiivi III peatüki artikkel 15 reguleerib intsidentidest teavitamist, tuleks IKT teavitamisele kohaldada CER direktiiv asemel DORA määrust.

Kuna DORA määruse artikli 19 lõike 6 punkt e kohaselt saab riik määrata, et lisaks punktides a–d nimetatud asutustele edastatakse tõsiste intsidentide teavitused ja raportid ka muudele liikmesriigi õiguse kohastele avaliku sektori asutustele, nähaksegi käesoleva lõikega 3 ette, et FI edastab viivitamata Eesti Pangale need teavitused ja raportid, mis ta on saanud elutähtsa teenuse osutajalt.

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 järelevalveasutus (kelleks on üks ESA-dest, sõltuvalt, kes on kriitilise tähtsusega kolmandast isikust IKT teenuseosutaja) aegsasti vastastikku kogu asjakohast teavet kriitilise tähtsusega kolmandast isikust IKT teenuseosutajate kohta, mida neil on vaja DORA määrusest tulenevate ülesannete täitmiseks, eelkõige seoses juhtiva järelevalveasutuse järelevalve 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 tavaid, hõlbustada koostööd, edendada tõlgendamise ühtsust ning anda lahkkelide korral jurisdiktsiooniüleseid hinnanguid.

FIS § 54 lõike 4 täiendamine uue punktiga 12. 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 § 54⁴ uue lõikega 4 võetakse riigisisesse 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 riigisisesse õigusesse üle võtta.

3.2. Eelnõu § 2. Finantskriisi ennetamise ja lahendamise seaduse muutmine

Digitaalne tegevuskerksus on oluline, et säilitada finantsasutuse kriitilised funktsioonid ja põhiariliinid kriisilahenduse korral ning seeläbi vältida häireid reaalmajanduses ja finantsüsteemis. 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 krediidasutusena ka investeerimisühingut ja tema suhtes kohaldatakse kõike krediidasutuse suhtes sätestatud, siis ka allolevaid selgitusi tuleks lugeda nii, et kõik, mis on öeldud krediidasutuse kohta, käib ka investeerimisühingu kohta. Samuti on oluline juhtida tähelepanu asjaolule, et FI on FELS-i mõttes kriisilahendusasutus. Kui FI-l, kui järelevalveasutusel, on krediidasutuse või investeerimisühingu kohta mingi teave tegelikult olemas, siis muudatuste kohaselt võib osutada vajalikuks teavitada FI-d, kui kriisilahendusasutust, samuti teatud asjaoludest. FIS § 4 lõike 4 kohaselt tagab FI vajalikus ulatuses finantsjärelevalve ja kriisilahendusülesannete funktsiooni omavahelise sõltumatus.

FELS § 2 lõike 2 muutmine (ei ole seotud DORA ülevõtmisega, seaduses parandatakse EL määruse nimetus õigeaks). 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 krediidasutuse finantsseisundi taastamise kava sisaldama. Muudatusega täpsustatakse sõnastust, et kava peab sisaldama muu hulgas korda ja meetmeid, tagamaks võrgu- ja infosüsteemide pidev toimimine. Võrgu- ja infosüsteemide 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 võrk³⁹; (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 14¹ ja 14². Lõige 5 kohustab krediidasutust 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 tehnoloogia teenuse 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 muutmise. Paragrahv 29 reguleerib, mida peab kriisilahenduskava sisaldama.

Punkti 5 kohaselt peab kava sisaldama informatsiooni selle kohta, millised on võimalused kriitiliste funktsioonide ja põhiariliinid õiguslikult ja majanduslikult teistest funktsioonidest eraldamiseks, et tagada krediidasutuse 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 KüTS § 2 punktis 1 sätestatud võrgu- ja infosüsteemide kirjelduse kohta (direktiivis on viide DORA määruses osutatud võrgu- ja infosüsteemidele, mis omakorda on defineeritud viitega NIS2 direktiivi määratlusele).

FELS § 33 lõike 4 punkti 4 muutmise ja täiendamine uue punktiga 4¹. Paragrahv 33 reguleerib, mida võetakse arvesse krediidasutuse ja konsolideerimisgrupi kriisilahenduskõlblikkuse hinnangu koostamisel.

Punktis 4 täpsustatakse, et kui hinnatakse krediidasutuse teenuslepingute täielikult täitmisele pööratavust krediidasutuse 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 4¹ kohaselt tuleb kriisilahenduskõlblikkuse hinnangu koostamisel võtta arvesse kriitilisi funktsioone ja põhiariliine toetavate võrgu- ja infosüsteemide digitaalsest tegevuskerksust. Selleks on abiks info- ja kommunikatsioonitehnoloogiaga seotud intsidentide

³⁹ „elektronilise side võrk“ – ülekandesüsteemid, mis võivad, aga ei pruugi põhineda püsitaristul või keskel juhtimisel, ja vajaduse korral lülitus- ja marsruutimiseseadmed 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, elektri kaabelsüsteeme, 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.

3.3. Eelnõu § 3. Hoiu-laenuühistute seaduse muutmine

Hoiu-laenuühistud kuuluvad vaikumisi DORA määruse kohaldamisalasse. Samas lubab DORA määruse artikli 2 lõige 4 riigisiselt 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 krediitiasutuste 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. Kui hoiu-laenuühistust saab ühistupank, siis viidatud eelnõu kohaselt kohalduksid neile KAS-is sätestatud nõuded, sh on nad kohustatud rakendama DORA määrust.

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 õigeaks). 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 kohaldamisele kuuluvad mh määratud väljamaksetega töödandja pensionifondid (IORP-id). Paragrahvis 223 on viited IFS paragrahvidele, milledes sätestatud peab ka IORP oma tegevuses arvestama. Muudatusega lisatakse §-i 223 viide IFS §-le 345, mille uus lõige 1¹ kohustab fondivalitsejaid järgima DORA määruses sätestatud. Lisaks on viide IFS uuele §-le 345¹ 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 nõuetega. Kuna DORA määrus ei kohaldu IORP-

ide suhtes, millesse kuulub vähem kui 15 pensioniskeemiga hõlmatud isikut, on õiguselguse 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 1¹ juures).

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

IFS § 345 uus lõige 1¹. Kuna fondivalitsejad kuuluvad samuti DORA kohaldamisalasse, on §-i 345 lisatud kohustus järgida DORA määruises sätestatud nõudeid, sealjuures peavad loodavad ja hallatavad võrgu- ja infosüsteemid vastama DORA määruises sätestatule.

Pensionifondide puhul ei ole tegemist eurofondi valitsejaga direktiivi 2009/65/EÜ artikli 2 lõike 1 punkti b tähenduses, mistõttu ei kuulu nad vaikumisi ka DORA määruise kohaldamisalasse. Eelnõu koostamisel on võetud lähenemine, et ka pensionifondid lähtuvad oma tegevuses DORA määruises sätestatud nõuetest, mistõttu on õiguselguse huvides sõnastuses ka nendele eraldi viidatud. Samas on täpsustatud, et mitte kõikide DORA määruise 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 määruise muutmisel tuleb kohaldatavad sätted pensionifondi valitsejate vaates uuesti riigisiselt 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 määruises (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 määruise (EL) 2022/2554 artiklites 3–18, artikli 19 lõigetes 1–5,

	artikli 22 lõikes 1, artiklites 24–30 ning artiklis 45 sätestatud.“;
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; - Nõuded finantsjärelevalve subjekti talitluspidevuse protsessi korraldamiseks.	IFS § 345 (1 ¹), artiklid 24–27.
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 § 345¹. 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 teavitatusvormi (**lõiked 1 ja 2**). Lõikega 1 nähakse ette, et fondivalitseja teavitab lisaks FI-le ka RIA-t.

Teavitused ja raportid intsidentide kohta tuleb esitada DORA määruse alamaktides kehtestatud vorme kasutades, lähtudes Finantsinspektsiooni kehtestatud andmevahetusvormingust ja teabe edastusviisist (vt tehniliste standardite eelnõu konsultatsioonidokumenti intsidentidest teavitamise kohta).⁴⁰ Nagu käesoleva seletuskirja punkti 2.3.2 alampunktis A kirjeldatud, kasutab finantsasutus nii FI kui ka RIA teavitamisel ühekordset teabeedastamise viisi ehk selle kehtestamisel tuleks Finantsinspektsioonil ka selle asjaoluga arvestada.

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

⁴⁰<https://www.eiopa.europa.eu/system/files/2023-12/JC%202023%2070%20-%20CP%20on%20draft%20RTS%20and%20ITS%20on%20major%20incident%20reporting%20under%20DORA.pdf>

kõnealuse teate edastada ka direktiivi (EL) 2022/2555 kohaselt määratud või loodud küberturbe intsidentide lahendamise üksustele.

IFS § 363¹ uus lõige 3. Selguse huvides on ka töandja 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 3². Paragrahv reguleerib järelevalve aluseid ja kohaldamist. Eelnõuga lisatakse paragrahvi uus lõige, milles sätestatakse, et FI-l on DORA määruse kohase täitmise üle järelevalve teostamisel kõik nimetatud määruses, IFS-is ja Finantsinspektsiooni seaduses sätestatud õigused.

Nimelt on DORA määruse artikli 50 lõike 1 kohaselt pädevatel asutustel kõik DORA määruse kohaste ülesannete täitmiseks vajalikud järelevalve-, uurimis- ja karistuste määramise volitused ning lõikes 2 on miinimumnimekiri vastavatest volitustest. 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 kontrollid või uurimisi ning nõuda määruse nõuete rikkumise korral parandus- ja ennetusmeetmete võtmist. Kuna tegemist on miinimumnimekirjaga, siis on Finantsinspektsioonil õigus rakendada ka muid IFS-is ja FISis sätestatud õigusi.

Finantsinspektsioonile antakse mh õigus rakendada DORA määruse artikli 50 lõikes 4 sätestatud halduskaristusi ja 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 (kuna liikmesriigi õigusega pole vastavat õigust ette nähtud, siis käesolevat meetet ei saa rakendada), ning
- avalike teadaannete väljastamine, mis sisaldavad füüsilise või juriidilise isiku identiteeti ja rikkumise laadi.

Kuna tegemist on jällegi miinimumnimekirjaga, on Finantsinspektsioonil õigus rakendada ka muid IFS-ist ja FIS-ist tulenevaid meetmeid.

Et võetud meetmetel oleks hoiatav mõju laiemale avalikkusele, näeb määrus ette rikkumist puudutavate otsuste avalikustamise. DORA määruse artikli 54 lõike 1 kohaselt avaldavad pädevad asutused oma ametlikel veebisaitidel põhjendamatu viivitusega kõik halduskaristuse määramise otsused, mida ei ole edasi kaevatud pärast seda, kui karistuse saanud isikut on otsusest teavitatud. Lõige 5 näeb samas ette, et kui pädev asutus avaldab halduskaristuse määramise otsuse, mis on asjaomastele kohtuasutustele edasi kaevatud, lisavad pädevad asutused ühtlasi viivitamata oma ametlikule veebisaidile selle teabe ja hiljem kogu täiendava teabe sellise edasikaebamise tulemuste kohta. Samuti avaldatakse kohtuotsus, millega tühistatakse halduskaristuse määramise otsus.

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.

Kuigi DORA määruse artikkel 54 viitab vaid halduskaristuste avalikustamisele, on eurofondi direktiivi 2009/65/EÜ artikli 99 lõikes 3 sätestatud, et liikmesriigid näevad ette, et pädevad asutused võivad avalikustada meetmed ja karistused, mis määratakse käesoleva direktiivi rakendamisel vastuvõetud sätete rikkumise korral, välja arvatud juhul, kui selline avalikustamine ohustaks tõsiselt finantsturge, kahjustaks investorite huve või tekitaks asjaomastele osalistele ebaproportsionaalset kahju. Kuna DORA nõuded integreeritakse viidatud direktiivi, on pädeval asutusel alus avalikustada lisaks halduskaristustele ka muud meetmed (nt ettekirjutus), kui rikutakse DORA nõudeid. Vastav õigus on FIS § 54 lõikes 5, mille kohaselt on Inspeksioonil õigus täielikult või osaliselt avalikustada väärtasjas tehtud lahend või haldusakt või -leping, kui see on ette nähtud käesoleva seaduse § 2 lõikes 1 nimetatud seaduses või kui see on vajalik investorite, finantsjärelevalve subjektide klientide või avalikkuse kaitseks või finantsturu õigus- või korrapärase toimimise tagamiseks.

IFS uus § 503⁴. 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 karistused 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 väärteto tulemusel teenitud kasule või ära hoitud kahjule vastavas summas ning juriidilise isiku korral karistatakse rahatrahviga kuni 5 000 000 eurot või kuni kahekordse väärteto tulemusel teenitud kasule või ära hoitud kahjule vastavas summas või kuni kümme protsenti juriidilise isiku või tema konsolideerimisgrupi konsolideeritud käibest.

Uue paragrahvi sätestamisel on lähtutud IFS-is sätestatud kehtivatest rahatrahvimääradest ja karistuste määramise alustest. Finantssektori karistusnormid on suures osas reguleeritud liidu õiguses, kus reeglina on ette nähtud analoogsed meetmed karistuste rakendamiseks (sh fikseeritud rahatrahvi piirmäärad). Kuna DORA määruse nõuded integreeritakse DORA direktiiviga vastavatesse finantssektori õigusaktidesse (eurofondi puhul direktiivi 2009/65/EÜ), on ka eelnõu puhul võetud lähenemine, et DORA nõuete rikkumise eest ette nähtud karistused oleksid kooskõlas vastavates liidu õigusaktides ette nähtud karistussätetega. IFS uue paragrahvi puhul on võetud aluseks direktiivi 2009/65/EÜ artikli 99 lõike 6 punktid e–g ja artikli 99a punkt j. DORA direktiiviga muudetakse 2009/65/EÜ direktiivi artiklit 12 nii, et sinna lisatakse viide DORA nõuete rakendamisele. Kuna 2009/65/EÜ direktiivi artikli 99a punkt j viitab artikli 12 rikkumisele, hõlmab see ühtlasi DORA nõuete rikkumist.

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, 3–5: 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 KindITS-is.

KindITS § 38 lõike 2 punkt 5 ja uus punkt 5¹ (ei ole seotud DORA direktiiviga, kuid on tehniline muudatus, et vältida seaduses olevat tühja viidet). Kuna ÄS § 386 lõike 2 punkt 4 on tunnustatud kehtetuks, korrigeeritakse KindITS sõnastust ja kustutatakse viide kehtetule ÄS punktile 4. ÄS-ist välja jäetud punkt sõnastatakse KindITS-is. Seega peab kolmanda riigi kindlustusandja Eestis filiaali asutamise loa taotlemisel esitama FI-le äriühingu põhikirja või ühingulepingu asukohamaa seaduste kohaselt tõestatud ära kirja, kui põhikirja või ühingulepingu registrile esitamine on nõutav ka ühingu asukohamaal.

KindITS § 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 KindITS-is viide määrusele kooskõlla selle õige nimega.

KindITS § 96 täiendamine uue lõikega 7¹. Kindlustusandja juhtimissüsteemi nõuete hulka kuulub ka DORA määruse rakendamine. Sealhulgas peab kindlustusandja kasutama ja haldama info- ja võrgusüsteeme vastavalt DORA määruses sätestatule.

KindITS § 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.

KindITS uus § 105¹. 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.

Teavitused ja raportid intsidentide kohta tuleb esitada DORA määruse alamaktides kehtestatud vorme kasutades, lähtudes Finantsinspeksiooni kehtestatud andmevahetusvormingust ja teabe edastusviisist (vt tehniliste standardite eelnõu konsultatsioonidokumenti intsidentidest teavitamise kohta).⁴¹ Nagu käesoleva seletuskirja punkti 2.3.2 alampunktis A kirjeldatud, kasutab finantsasutus nii FI kui ka RIA teavitamisel ühekordset teabeedastamise viisi ehk selle kehtestamisel tuleks Finantsinspeksioonil ka selle asjaoluga arvestada.

⁴¹<https://www.eiopa.europa.eu/system/files/2023-12/JC%202023%2070%20-%20%20CP%20on%20draft%20RTS%20and%20ITS%20on%20major%20incident%20reporting%20under%20DORA.pdf>

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**).

KindlITS § 138 muutmine (ei ole seotud DORA direktiiviga). Paragrahvi lisatakse uus lõige, mille kohaselt ei ole kindlustusandjate (v.a Euroopa äriühingud) piiriülene ümberkujundamine lubatud. Piiriülene ümberkujundamine tähendab, et Eesti äriühingu saab ümber kujundada lepinguriigi äriühinguks.

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 krediitvahendustevõtjaid ja teisi finantsettevõtjaid, ega vastavalt kõnealusele liidu õigusele kehtestatud liikmesriigi õigusnormide kohaldamist. Kindlustustegevust reguleeriva Euroopa Parlamendi ja nõukogu direktiivi 2009/138/EÜ peaesmärk on kindlustusvõtjate ja soodustatud isikute asjakohane kaitse (põhjenduspunkt 14). Direktiivis ettenähtud kindlustustegevuse loarežiimiga tagab, et kindlustusturul tegutsevad usaldusväärsed ja jätkusuutlikud kindlustusandjad, kes on suutelised täitma kindlustuslepingutest tulenevaid kohustusi. Luba annab kindlustusandjale õiguse tegutseda piiriüleselt Euroopa passi alusel.

Seega, arvestades, et finantssektoris teenuse osutamiseks peab isikul olema tegevusluba, mille ta saab asukohariigi finantsjärelevalve asutuselt, ei ole direktiiviga 2009/138/EÜ kooskõlas olukord, kus kindlustusandja liigub oma tegevuse ja kindlustusportfelliga teise lepinguriiki, kus tal puudub vastava lepinguriigi finantsjärelevalve asutuse luba selles riigis kindlustusteenuse osutamiseks. Samas ei ole tal võimalik tegevusluba taotleda, kui ta on samal ajal (veel) Eesti registrisse kuuluv äriühing, kellel on Eestis kehtiv tegevusluba olemasoleva kindlustusportfelli teenindamiseks. Kindlustusportfelli ei ole võimalik vahepealseks perioodiks, kui kindlustusandja uues liikmesriigis tegevusluba taotleb, ootele panna, jättes samal ajal teenindamata kõik kindlustusvõtjate, kindlustatute ja soodustatud isikute nõuded ja tegemata väljamakseid kahjustatud isikutele (teatud juhtudel on ajakriitiline, et kindlustusandja reageerib viivitamata kindlustusjuhtumisele, nt seoses tervisekindlustusega). Sealjuures on teise liikmesriigi pädeval asutusel õigus tegevusloa andmisest ka keelduda.

Alternatiiv on asutada lepinguriigis uus äriühing, saada selle lepinguriigi järelevalveasutuselt tegevusluba kindlustusteenuse osutamiseks, misjärel Eesti kindlustusandja saab selle ühinguga ühineda või talle kindlustusportfelli üle anda. Sellisteks olukordadeks on KindlITS ette nähtud ka vastav regulatsioon klientide kaitseks. Näiteks võib KindlITS § 161 lõike 1 kohaselt kindlustusandja vabatahtlikult lõpetada üksnes tingimusel, et kindlustusportfell on kehtestatud korras üle antud, kindlustuslepingud lõpetatud või kõik kindlustuslepingutest tulenevad kohustused täidetud ning tema varad on piisavad kõigi võlausaldajate õigustatud nõuete täielikuks rahuldamiseks. Kindlustusandja ühinemisel teise lepinguriigi kindlustusandjaga tagatakse samuti kindlustusvõtjate, kindlustatute ja soodustatud isikute kaitse see läbi, et ühinemiseks on vaja Finantsinspektsiooni luba. KindlITS § 144 lõike 2 punkti 5 kohaselt võib Finantsinspektsioon keelduda ühinemisloa andmisest, kui ühinemine võib kahjustada kindlustusvõtjate, kindlustatute või soodustatud isikute õigustatud huve.

Nagu eelpool osutatud, ei ole piiriülese ümberkujundamise puhul võimalik tagada, et kindlustusandja liigub teise liikmesriiki ning tal on selles teises liikmesriigis juba olemas tegevusluba, et koheselt jätkata klientide ees kohustuste täitmist. Selline liikumine ei ole kooskõlas direktiivi 2009/138/EÜ tegevusloa režiimi ja peaesmärgi ehk kindlustusvõtjate ja soodustatud isikute asjakohase kaitsega.

Kuigi direktiiv (EL) 2019/2121 näeb ette meetmed võlausaldajate kaitseks, ei ole direktiiviga tagatud piisav kliendikaitset juhuks, kui äriühing selles teises liikmesriigis tegevuse jätkamiseks tegevusluba ei saa (teise riiki liikumine ei tähenda automaatselt liidu õigusest tuleneva tegutsemisõiguse (tegevusloa) üleminekut). ÄS § 491⁸ reguleerib võlausaldajate kaitset, kuid tagatise saamise õigus on vaid võlausaldajal, kelle nõuded on tekkinud enne piiriülese ümberkujundamise projekti avalikustamist, ja nõuete osas, mis ei ole muutunud avalikustamise kuupäevaks sissenõutavaks. Direktiivi ülevõtmise eelnõu seletuskirjas⁴² on selgitatud, et liikmesriigil tuleb tagada selliste võlausaldajate kaitse, kelle nõuded tekkisid enne piiriülese ümberkujundamise otsuse projekti avalikustamist ja need ei ole avalikustamise kuupäevaks veel sissenõutavaks muutunud. Liikmesriigid peavad tagama, et võlausaldajad, kes ei ole rahul tagatistega, mida pakutakse piiriülese ümberkujundamise otsuse projektis, võivad taotleda asjakohaselt haldus- või kohtuorganilt piisavaid tagatise kolme kuu jooksul alates piiriülese ümberkujundamise otsuse projekti avalikustamisest, kui võlausaldajad suudavad usaldusväärset näidata, et nende nõuete rahuldamine on piiriülese ümberkujundamise tõttu ohus ja nad ei ole saanud äriühingult piisavaid tagatise. Tagatised peavad sealjuures olema tingimuslikud, st sõltuma sellest, kas piiriülene ümberkujundamine ikkagi jõustub.

Siinjuures tasub meeles pidada, et käesoleval juhul on võlausaldajateks kindlustusvõtjad, kindlustatud ja soodustatud isikud, kellele ei pruugi olla piisavalt teadlikust tagatist nõuda või haldus- või kohtuorgani poole pöörduda. Seega kindlustusvõtjate ja kindlustatute kaitse seisukohast ei ole võimalik tagada, et piiriülese ümberkujundamise korral oleks viidatud isikute huvid piisavalt kaitstud.

KindlITS § 175 lõike 1 muutmine. Kuna DORA määrus kohaldub ka kindlustusvahendajatele, sealhulgas §-s 175 defineeritud kõrvalvahendajatele, on § 175 lõikesse 1 lisatud viide uuele §-le 181¹, milles reguleeritakse, et kindlustusvahendajatele kohalduvad digitaalse tegevuskerksuse nõudeid.

KindlITS § 179 lõike 1 punkti 2 muutmine (ei ole seotud DORA direktiiviga, kuid on seotud EL õiguse rakendamisega). Paragrahv 179 lõikes 1 kohaselt peab vahendaja sõlmima kindlustuse turustamisest tuleneva kohustuse rikkumisega tekitatud kahju hüvitamise tagamiseks kohustusliku vastutuskindlustuslepingu ning sama lõike punktides 1–5 on sätestatud miimumnõuded, mis tingimustele see leping peab vastama. Punkti 2 kohaselt peab kindlustussumma olema vähemalt 1 300 380 eurot ühe kindlustusjuhtumi kohta ja 1 924 560 eurot aastas kõigi esitatud nõuete kohta. Viidatud piirmäärade aluseks on kindlustusturustuse direktiivi⁴³ artikli 10 lõige 4. Eelnõus esitatud muudatuse aluseks on sama artikli lõige 7, mille kohaselt vaatab EIOPA vastutuskindlustuse summad korrapäraselt läbi, et võtta arvesse muutusi Eurostati avaldatavas Euroopa tarbijahinnaindeksis ning esitab komisjonile regulatiivsete tehniliste standardite eelnõu uute piirmäärade kehtestamiseks. Lõike 7 kohaselt vaadati esimest korda määrad üle 31. detsembriks 2017 ning edaspidi toimub see iga viie aasta järel.

⁴² <https://www.riigikogu.ee/tegevus/eelnoud/eelnou/75cf6d3f-bcfe-436e-bd51-3a1333c185ad/ariseadustiku-muutmise-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus-ariuhingute-piiriulene-liikumine>

⁴³ Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/97, mis käsitleb kindlustustoodete turustamist.

30. juunil 2023 esitas EIOPA komisjonile regulatiivsete tehniliste standardite eelnõu, millega kohandatakse baassummasid vastavalt direktiivi (EL) 2016/97 artikli 10 lõikele 7 (vaatlusalune periood oli 1. jaanuarist 2018. a kuni 31. detsembrini 2022. a). Kuna viidatud perioodil muutus indeks 20,32%, muudetakse vastutuskindlustuse summasid järgmiselt:

	Kehtiv summa (EUR)	Uus summa [muutus] (EUR)
Kindlustussumma ühe juhtumi kohta	1 300 380	1 564 610 [+264 230]
Kindlustussumma aastas kõigi esitatud nõuete kohta	1 924 560	2 315 610 [+391 050]

Seoses eeltooduga viiakse ka § 179 kindlustussummad vastavusse uute EL õigusest tulenevate uute baassummadega.

KindlITS uus § 181¹. 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 105¹ sätestatud, kindlustusvahendajad peavad teavitama nii FI-d kui ka RIA-t tõsistest IKT-ga seotud intsidentidest.

KindlITS § 186 lõike 2 punkti 13 muutmise. Kindlustusmaakleri sise-eeskirjade puhul täpsustatakse, et kui kindlustusmaaklerile kohaldu 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.

KindlITS § 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 KindlITS sõnastust ja kustutatakse viide kehtetule ÄS punktile 4. ÄS-ist välja jäetud punkt sõnastatakse KindlITS-is. Seega peab kolmanda riigi kindlustusvahendaja Eestis filiaali asutamise loa taotlemisel esitama FI-le äriühingu põhikirja või ühingulepingu asukohamaa seaduste kohaselt tõestatud ära kirja, kui põhikirja või ühingulepingu registreile esitamine on nõutav ka ühingu asukohamaal.

KindlITS § 224 uus lõige 3. Paragrahv reguleerib järelevalve ülesandeid ja õigusi. Eelnõuga lisatakse paragrahvi uus lõige, milles sätestatakse, et FI-l on DORA määruse kohase täitmise üle järelevalve teostamisel kõik nimetatud määruses, KindlITS-is ja FIS-is sätestatud õigused. Nimelt on DORA määruse artikli 50 lõike 1 kohaselt pädevatel asutustel kõik DORA määruse kohaste ülesannete täitmiseks vajalikud järelevalve-, uurimis- ja karistuste määramise volitused ning lõikes 2 on miinimumnimekirja volitustest. 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 kontrollid või uurimisi ning nõuda määruse nõuete rikkumise korral parandus- ja ennetusmeetmete

võtmist. Kuna tegemist on miinimumnimekirjaga, siis on Finantsinspeksioonil õigus rakendada ka muid KindlITS-is ja FISis sätestatud õigusi.

Finantsinspeksioonile antakse mh õigus rakendada DORA määruse artikli 50 lõikes 4 sätestatud halduskaristusi ja 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 (kuna liikmesriigi õigusega pole vastavat õigust ette nähtud, siis käesolev meedet ei saa rakendada), ning
- avalike teadaannete väljastamine, mis sisaldavad füüsilise või juriidilise isiku identiteeti ja rikkumise laadi.

Kuna tegemist on jällegi miinimumnimekirjaga, on FI-l õigus rakendada ka muid KindlITS-ist ja FIS-ist tulenevaid meetmeid.

Et võetud meetmetel oleks hoiatav mõju laiemale avalikkusele, näeb määrus ette rikkumist puudutavate otsuste avalikustamise. DORA määruse artikli 54 lõike 1 kohaselt avaldavad pädevad asutused oma ametlikel veebisaitidel põhjendamatu viivitusega kõik halduskaristuse määramise otsused, mida ei ole edasi kaevatud pärast seda, kui karistuse saanud isikut on otsusest teavitatud. Lõige 5 näeb samas ette, et kui pädev asutus avaldab halduskaristuse määramise otsuse, mis on asjaomastele kohtuasutustele edasi kaevatud, lisavad pädevad asutused ühtlasi viivitamata oma ametlikule veebisaidile selle teabe ja hiljem kogu täiendava teabe sellise edasikaebamise tulemuste kohta. Samuti avaldatakse kohtuotsus, millega tühistatakse halduskaristuse määramise otsus.

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 väärtemenetlust, 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.

Kuigi DORA määruse artikkel 54 viitab vaid halduskaristuste avalikustamisele, on FI-l õigus FIS § 54 lõike 5 kohaselt avalikustada lisaks väärteto asjas tehtud lahendile haldusakt või -leping, kui see on vajalik investorite, finantsjärelevalve subjektide klientide või avalikkuse kaitseks või finantsturu õigus- või korrapärase toimimise tagamiseks.

KindlITS uus § 257¹ 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 700 000 eurot või kuni

kahekordse väärteto tulemusel teenitud kasule või ära hoitud kahjule vastavas summas ning juriidilise isiku korral karistatakse rahatrahviga kuni 5 000 000 eurot või kuni kahekordse väärteto tulemusel teenitud kasule või ära hoitud kahjule vastavas summas või kuni kümme protsenti juriidilise isiku või tema konsolideerimisgrupi konsolideeritud käibest. Määrade kehtestamisel on lähtutud §-s 257 sätestatud juhtimissüsteemi määradest.

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, 3–5: 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.

KindITS § 263³ muutmise (ei ole seotud DORA direktiiviga). Kuna paragrahv ei koosne lõigetest, kustutatakse paragrahvist tekstiosa „käesoleva lõike“ ning „esimese lause“ asemel on viide „eelmisele lausele“.

Seaduse normitehniline märkus. Muudatusega lisatakse viide DORA direktiivile.

3.6. Eelnõu § 6. Krediidiandjate ja -vahendajate seadus

KAVS § 28 lõike 5 muutmise (ei ole seotud DORA direktiiviga, seaduses parandatakse EL määruse nimetus õigeaks). 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.

3.7. Eelnõu § 7. Krediidiasutuste seaduse muutmise

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 jälgiks 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 ilmnunud panga poolt DORA määruse alusel läbi viidud digitaalse tegevuskerksuse testimise käigus.

KAS § 20⁶ 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 Eesti 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 krediidasutuse poolt lubatud. ÄS § 384 lõike 1 muudatust on selgitatud⁴⁴ 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 piiriülevalt 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 muutmise 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 krediidasutus 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 § 82⁴. Seadusesse lisatakse eraldi paragrahv operatsiooniriski juhtimise nõuete sätestamiseks. Krediidasutuse riskijuhtimise nõuete hulka kuulub mh DORA määruse rakendamine. Sealhulgas peavad krediidasutus info- ja võrgusüsteemid olema loodud ja hallatud vastavalt DORA määruses sätestatule.

Kui KAS § 82 lõige 5 sätestab, et krediidasutus peab kõigi oluliste äriprotsesside kohta välja töötama talitluspidevuse plaani majandustegevuse taastamise ja jätkuvuse tagamiseks, siis § 82² 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 taasteplaanide on vaja selleks, et krediidasutus 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 krediidasutus kõiki funktsioone toetavate IKT-süsteemide IKT talitluspidevuse plaane ning IKT reageerimis- ja taasteplaanide 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 krediidasutuse 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 digitaalse tegevuskerksuse testimise, teabevahetuse kokkulepete ja kolmandatest isikutest tulenevat IKT-riskide kohta. Seega, muudatusettepaneku kohaselt ei kohaldata krediidasutustele KütS 2. peatükki. Samuti ei kohaldata HOS sätet (§ 41 lg 1), mis viitab KütS §-dele 7 ja 8, mis kuuluvad KütS 2. peatükki, kuid mida, nagu eelpool osutatud, krediidasutuste suhtes ei kohaldata.

⁴⁴ Äriseadustiku ja raamatupidamise seaduse muutmise seaduse (digilahendused äriühinguõiguses) eelnõu seletuskiri

KAS uus § 92³. 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 3**). Lõikega 1 nähakse ette, et krediidasutus teavitab lisaks FI-le ka RIA-t. Teavitused ja raportid intsidentide kohta tuleb esitada DORA määruse alamaktides kehtestatud vorme kasutades, lähtudes Finantsinspeksiooni kehtestatud andmevahetusvormingust ja teabe edastusviisist (vt tehniliste standardite eelnõu konsultatsioonidokumenti intsidentidest teavitamise kohta).⁴⁵ Nagu käesoleva seletuskirja punkti 2.3.2 alampunktis A kirjeldatud, kasutab finantsasutus nii FI kui ka RIA teavitamisel ühekordset teabeedastamise viisi ehk selle kehtestamisel tuleks Finantsinspeksioonil ka selle asjaoluga arvestada.

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.

Lõige 3. Selleks, et mitte kohaldada krediidasutustele, kes on elutähtsa teenuse osutajad HOS § 38 lõike 1 tähenduses, topelt teavitamise nõuded, loetakse DORA kohase teavitusega HOS § 38 lõike 3 punktis 4 sätestatud elutähtsa teenuse osutaja teavitamise kohustus täidetuks, kui tegemist on tõsise IKT intsidendiga. Selguse tagamiseks on lisatud lõikesse ka täpsustus, et kui HOS § 37 lõike 3 punktis sätestatud sündmus ei liigitu tõsiseks IKT intsidentid, mis tähendab, et sellest teavitamisele ei kohaldu ka DORA kohased teavitamise nõuded, kohaldub sellisest sündmusest teavitamisele HOS ja selle § 37 lõike 2 alusel kehtestatud määrus. Vt selgitust ka FIS 47¹¹ lõike 3 juures.

Lõige 4. 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 krediidasutuse rakendatavad strateegiad, juhtimise korraldus, protseduurid, sealhulgas raamatupidamises rakendatavad protseduurid, aruandlussüsteemid ja sisekontroll on kooskõlas Euroopa Parlamendi ja nõukogu määruse (EL) nr 575/2013, krediidasutuste seaduse ja muude õigusaktide nõuetega, selleks, et usaldusväärset hinnata riske, sealhulgas süsteemset riski, digitaalse tegevuskerksuse testimise käigus ilmnenu riski ja stressitesti käigus ilmnenu 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

⁴⁵<https://www.eiopa.europa.eu/system/files/2023-12/JC%202023%2070%20-%20CP%20on%20draft%20RTS%20and%20ITS%20on%20major%20incident%20reporting%20under%20DORA.pdf>

juhtimise ja piisava katmise, käib see ka digitaalse tegevuskerksuse testimise käigus ilmnenu riskide kohta. Seega hindab FI § 96 lõike 5 kohaselt ka digitaalse tegevuskerksuse testimise käigus tuvastatud riskide puhul, kas likviidsus ja omavahendid on piisavad krediitiasutuse 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 4¹ eraldi välja toodud, et selliseks isikuks on ka IKT-teenuseosutaja.

KAS § 103 uus lõige 3². Paragrahv reguleerib ettekirjutuse tegemist ja muude meetmete rakendamist. Eelnõuga lisatakse paragrahvi uus lõige, milles sätestatakse, et FI-l on DORA määruse kohase täitmise üle järelevalve teostamisel kõik nimetatud määruses, KAS-is ja FIS-is sätestatud õigused.

Nimelt on DORA määruse artikli 50 lõike 1 kohaselt pädevatel asutustel kõik DORA määruse kohaste ülesannete täitmiseks vajalikud järelevalve-, uurimis- ja karistuste määramise volitused ning lõikes 2 on miinimumnimekirja volitustest. 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 kontrollid või uurimisi ning nõuda määruse nõuete rikkumise korral parandus- ja ennetusmeetmete võtmist. Kuna tegemist on miinimumnimekirjaga, siis on Finantsinspeksioonil õigus rakendada ka muid KAS-is ja FIS-is sätestatud õigusi.

Finantsinspeksioonile antakse mh õigus rakendada DORA määruse artikli 50 lõikes 4 sätestatud halduskaristusi ja 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 (kuna liikmesriigi õigusega pole vastavat õigust ette nähtud, siis käesolev meedet ei saa rakendada), ning
- avalike teadaannete väljastamine, mis sisaldavad füüsilise või juriidilise isiku identiteeti ja rikkumise laadi.

Kuna tegemist on jällegi miinimumnimekirjaga, on FI-l õigus rakendada ka muid KAS-ist ja FIS-ist tulenevaid meetmeid.

Et võetud meetmetel oleks hoiatav mõju laiemale avalikkusele, näeb määrus ette rikkumist puudutavate otsuste avalikustamise. DORA määruse artikli 54 lõike 1 kohaselt avaldavad pädevad asutused oma ametlikel veebisaitidel põhjendamatu viivitusega kõik halduskaristuse määramise otsused, mida ei ole edasi kaevatud pärast seda, kui karistuse saanud isikut on otsusest teavitatud. Lõige 5 näeb samas ette, et kui pädev asutus avaldab halduskaristuse määramise otsuse, mis on asjaomastele kohtuasutustele edasi kaevatud, lisavad pädevad

asutused ühtlasi viivitamata oma ametlikule veebisaidile selle teabe ja hiljem kogu täiendava teabe sellise edasikaebamise tulemuste kohta. Samuti avaldatakse kohtuotsus, millega tühistatakse halduskaristuse määramise otsus.

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.

Nii DORA määruse artikkel 54 kui ka krediidasutuste direktiivi 2013/36/EL artikkel 68 viitavad halduskaristuste avaldamisele, kuid FIS § 54 lõige 5 annab FI-le õiguse avalikustada täielikult või osaliselt nii väärteoasjas tehtud lahend kui ka haldusakt või -leping, kui see on vajalik investorite, finantsjärelevalve subjektide klientide või avalikkuse kaitseks või finantsturu õigus- või korrapärase toimimise tagamiseks.

KAS §-de 134²³–134²⁵ 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 140¹–140³.

KAS uus § 134²⁶. 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 sätestamisel on lähtutud KAS-is sätestatud kehtivatest karistusmääradest ja karistuste määramise alustest. Finantssektori karistusnormid on suures osas reguleeritud liidu õiguses, kus reeglina on ette nähtud analoogsed meetmed karistuste rakendamiseks (sh fikseeritud rahatrahvi piirmäärad). Kuna DORA määruse nõuded integreeritakse DORA direktiiviga vastavatesse finantssektori õigusaktidesse (krediidasutuste puhul direktiivi 2013/36/EL), on ka eelnõu puhul võetud lähenemine, et DORA nõuete rikkumise eest ette nähtud karistused oleksid kooskõlas vastavates liidu õigusaktides ette nähtud karistussätetega. KAS uue paragrahvi puhul on võetud aluseks 2013/36/EL direktiivi artikli 67 lõike 1 punkt d ja lõike 2 punktid e–g. DORA direktiiviga muudetakse 2013/36/EL direktiivi artiklit 74 nii, et sinna lisatakse viide DORA nõuete rakendamisele. Kuna 2013/36/EL direktiivi artikli 66 lõike 1 punkt d viitab artikli 74 rikkumisele, hõlmab see ühtlasi DORA nõuete rikkumist.

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, 3–5: 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. Muudatus on normitehniline. 2002. aastal⁴⁶ tunnistati kehtetuks KAS §-d 135–140, mistõttu on kehtetuks tunnistatud §-de 134²³–134²⁵ uuesti sõnastamisel kasutatud numeratsiooni 140¹ ja 140², vältimaks, et iga kord peab samad paragrahvid uuesti kehtetuks tunnistama ja uuesti kehtestama, kui on soov lisada vastutuse peatükki uued karistuse paragrahvid.

Finantssektori väärtegade kolmeaastased aegumistähtjad nähti ette finantsvaldkonna väärtekaristuste reformi raames. Paralleelselt menetleti JuMi vastutusvaldkonda kuuluvat karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadust (Euroopa Liidu õigusest tulenevad rahatrahvid), mille seletuskirjas on selgitatud, et „väljatöötamiskavatsuse kooskõlastamisel avaldati arvamust, et kõrgema rahatrahvi ülemmääraga karistatavate väärtegade korral tuleks sätestada senisest pikem aegumistähtaeg. Eelnõu koostamisel leiti algselt, et kuna kehtiv õigus võimaldab teatud väärtegade korral sätestada kaheaastase aegumistähtaja asemel kolmeaastase aegumistähtaja (KarS § 81 lg 3) ning suurema ebaõigussisuga teise astme kuritegu aegub viie aastaga (KarS § 81 lg 1 p 2), ei ole praegu erisuse loomine vajalik. Sellegipoolest leiti ka eelnõu kooskõlastamisel esitatud arvamustes jätkuvalt, et väärtegade üldine aegumistähtaeg ei võimalda finants- ja andmekaitse valdkonnas väärteomenetlusi tõhusalt läbi viia, arvestades nendes valdkondades toime pandavate väärteegade keerukust“. Teise lugemise seletuskirjas on lisaks, et „esimese lugemise läbinud eelnõus ei nähtud ette väärtegade aegumistähtaja pikendamist, vaid sätestati täiendavad aegumise katkemise alused. Arvestades siiski teatud valdkondade eripära, võib senisest suuremate trahvide korral olla põhjendatud ka pikemate aegumistähtaegade sätestamine. Nii näiteks on EL määruse (EU) 468/2014 artikli 130 kohaselt Euroopa Keskpanga poolt kohaldatavate trahvide korral aegumistähtjaks 5 aastat. Kui krediidiastutus ei allu Euroopa Keskpanga järelevalvele, oleks Eestis sama rikkumise korral aegumistähtaeg põhjendamatult lühem. Kehtiv KarS § 81 lg 3 näeb ette, et üldreeglina on väärte aegumistähtaeg 2 aastat ning seaduses sätestatud juhtudel võib ette näha kolmeaastase aegumistähtaja. Ettepaneku kohaselt jääks KarS § 81 lg 3 üldreegliks 2 aastat, kuid seaduses võib ette näha ka kuni 5-aastase aegumistähtaja (so kolme-, nelja- või viieaastase aegumistähtaja). Arvestades siiski, et 5-aastane aegumistähtaeg on ka teise astme kuriteo aegumistähtjaks, peaks nii pikk aegumistähtaeg väärtegade korral olema siiski erandlik.“.

Finantsvaldkonnas võib olla tegemist väga keeruliste kaasustega, mis on tavaliselt nn peitsüüteod (nagu näiteks ka maksustamise valdkonna süüteod), s.t. rikkumise toimepanemise asjaolud ei ole kergelt märgatavad, kannatanud ei ole või tema isik ei ole teada ja süüteo toimepannud isik teeb kõik endast oleneva, et järelevalveasutus ei avastaks rikkumist.

Seaduse normitehniline märkus. Muudatusega lisatakse viide DORA direktiivile.

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

Direktiivis (EL) 2015/2366 on sätestatud erinormid IKT turvalisuskontrollide ja riskimaanduselementide kohta seoses makseteenuste osutamiseks tegevusloa saamisega. Loa

⁴⁶ <https://www.riigiteataja.ee/akt/212735>

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 osahinguna, kuigi makseasutus peab samade teenuste osutamiseks olema aktsiaselts.

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 1¹ 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 § 17 lõike 5 muutmine (ei ole DORA direktiivi ülevõtmine, muudatusega täpsustatakse kehtivat õigust). MERAS § 17 lõige 5 sätestab, et FI võib jätta tegevusloa taotluse läbi vaatamata, kui taotleja ei ole kõrvaldanud puudusi ettenähtud tähtaja jooksul või ei ole esitanud tähtpäevaks nõutud andmeid ja dokumente. Muudatusettepanekuga laiendatakse taotluse läbi vaatamata jätmise võimalust ka olukorrale, kus taotlus on esitatud oluliste puudustega. Lisaks kustutatakse lõike teine lause.

MERAS § 24 lõike 3 muutmine ja täiendamine uue lõikega 4¹ (ei ole seotud DOA direktiiviga). MERAS sätted, mis reguleerivad piiriülest makseteenuse osutamist kolmandas riigis, on ebaselged ja puudulikud, mistõttu on FI-l takistatud selliste taotluste menetlemine, mille puhul soovitakse teenust osutada kolmandas riigis. MERAS § 24 lõike 3 kehtiva sõnastuse kohaselt kohaldatakse Eesti makseasutuse ja e-raha asutuse poolt kolmandas riigis teenuste osutamisele MERAS §-des 25-28, § 29 lõigetes 1, 2, 8 ja 10 ning § 92 lõigetes 11 ja 12 sätestatud. MERAS §-d 25–28 reguleerivad kolmandas riigis filiaali asutamist. Piiriüleselt teenuse osutamisele kohaldatakse § 29 lõigetes 1, 2, 8 ja 10 sätestatud. Paragrahv 29 reguleerib teises lepinguriigis filiaali asutamist ja piiriüleselt teenuse osutamist. Lõike 1 kohaselt tuleb FI-le esitada andmed ja dokumendid (lõike 2 kohaselt eesti keeles). Ükski järgnev viidatav säte ei reguleeri, mida FI peab talle esitatud andmete ja dokumentidega tegema. Samas ei ole

asjakohane reguleerida kolmanda riigi järelevalveasutusega suhtlust (andmete ja dokumentide edastamist ja sihtriigi järelevalveasutuselt hinnangu saamist), kuna see ei pruugi olla kooskõlas kolmanda riigi õigusega. Lõike 8 teine lause viitab läbi lõike 6 punkti 1, et FI peab heakskiidu andma, aga samas nimetatud heakskiidu aluseks on MERAS § 29 lõike 6 kohaselt „sihtriigi finantsjärelevalve asutuse hinnang“, mille saamine, nagu osutatud, ei ole rakendatav, kui FI pole sihtriigi järelevalveasutusele hinnangu saamiseks andmeid ja dokumente edastanud.

Muudatusettepanekuga nähakse ette, et kolmandas riigis piiriüleselt teenuse osutamiseks peab makseasutusel ja e-raha asutusel olema selles riigis tegutsemise luba ning selle taotlemisele, menetlemisele, andmisele ja kehtetuks tunnistamisele kohaldatakse samu reegleid, mis on ette nähtud kolmandas riigis filiaali asutamisele. Samas, § 25 lõike 2 asemel tuleb FI-le esitada § 29 lõike 1 punktides 1 ja 2 nimetatud andmed ja dokumendid. Seega tuleb äriplaani asemel esitada tegevuskava, mis sisaldab andmeid kõigi sihtriigis osutatavate teenuste kohta. Kuna äriplaani asemel esitatakse tegevuskava, siis § 27 punktides 3 ja 4 äriplaani kohta sätestatud tuleks kohaldada tegevuskava suhtes. Ehk FI võib keelduda filiaali asutamise loa andmisest, kui makseasutuse või e-raha asutuse finantsseisund, organisatsiooniline ülesehitus ja muud võimalused ei ole piisavad tegevuskavas nimetatud teenuste osutamiseks kolmandas riigis või kui tegevuskava rakendamine võib kahjustada makseasutust või e-raha asutust, tema aktsionäride huve, makseasutuse või e-raha asutuse finantsseisundit või tegevuse usaldusväärsust Eestis, teises lepinguriigis või kolmandas riigis.

MERAS § 32 lõike 2 punkti 6 muutmise ja uus punkt 6¹ (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 § 44 lõike 1 punkti 3 muutmise (ei ole seotud DORA direktiiviga). Muudatusega parandatakse seaduses olev ekslik viide. Õige on viidata § 54 asemel §-le 39, mis reguleerib olulise osaluse omandamisest FI teavitamist.

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

MERAS § 50 lõike 3 punkti 9 muutmise. Makseasutuses ja e-raha asutuses peab siseeskirjadega 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 muutmise. Kehtivasse sõnastusse on lisatud viide DORA määrusele, milles sätestatud tuleb arvesse võtta info- ja kommunikatsioonitehnoloogia talitluspidevuse põhimõtete ja plaanide ning info- ja kommunikatsioonitehnoloogia reageerimis- ja taastepaanide koostamisel ja kehtestamisel, testimisel ja läbivaatamisel.

Tõhusaid talitluspidevuse ja taasteplaane on vaja selleks, et makseasutus saaks kohe ja kiiresti lahendada IKT intsidentid, 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 varurajatist.

MERAS § 52 muutmise (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 osutamise 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 1¹. Osaühinguna asutatud asutuse ümber kujundamiseks aktsiaseltsiks peab ettevõtja järgima muu hulgas äriseadustikus sätestatud nõudeid ja kohandama ettevõtte tegevuse vastavaks.

Lõikes 1² 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 1³ 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 1⁴ 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, näiteks äriseadustikus, sätestatud nõuetele (punkt 2). Kui ümberkujundamine võib muul põhjusel kahjustada klientide huve (punkt 3), on FI-l samuti õigus keelduda ümberkujundamise loa andmisest. Näiteks võib ümberkujundamine kahjustada klientide huvi, kui ümberkujundamise protsessi tõttu langeb teenuse kvaliteet või kättesaadavus või toob klientidele kaasa lisakulusid, mistõttu on oluline, et makseasutuse ja e-raha asutused rakendaksid ümberkujundamisprotsessi hoolikalt ja klientide huve arvestades. 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. Äriühingu ümberkujundamine võib kaasa tuua mitmeid õiguslikke küsimusi, sealhulgas seoses lepingute ja kohustustega, kahjustades teiste osapoolte õigusi või tekitades ebakindlustust, mistõttu on oluline, et järelevalveasutuse õigused keelduda ümberkujundamise loa andmisest ei oleks väga kitsalt piiritletud ning ta saaks hinnata ümberkujundamise mõju seoses õiguslike küsimuste, turukonkurentsi, finantsstabiilsuse säilitamise ja tarbijakaitse tagamise vaates laiemalt.

Lõike 1⁵ kohaselt avalikustab FI ümberkujundamisloa andmise otsuse hiljemalt otsuse tegemisele järgneval tööpäeval oma veebilehel.

Lõige 1⁶ sätestab, et äriregistrile esitatavale avaldusele lisatakse FI luba teenuseosutaja ümberkujundamiseks, millest tulenevalt on vajalik saada FI luba enne ümberkujundamise lõpuleviimist äriregistri kandega.

Lõige 1⁷. Kuigi eelnõuga muudetakse makseasutuse ja e-raha asutuste ümberkujundamist paindlikumaks, siis piiriülene ümberkujundamine ei ole jätkuvalt lubatud (ehk eelnõuga seda ei muudeta), kuna piiriülese ümberkujundamisega ei ole tagatud piisav klientide huvide kaitse.

Direktiivi (EL) 2019/2121 põhjenduspunkti 57 kohaselt ei tohiks viidatud direktiiv mõjutada liidu õiguse kohaldamist, mis reguleerib kredidivahendustevõtjaid ja teisi finantsettevõtjaid, ega vastavalt kõnealusele liidu õigusele kehtestatud liikmesriigi õigusnormide kohaldamist. Makseasutuste tegevust reguleeriva direktiivi (EL) 2015/2366 põhjenduspunkti 6 kohaselt on direktiivi eesmärgiks tagada kõrgetasemeline tarbijakaitse kogu liidu makseteenuste kasutajatele. Selle tagamise üheks meetmeks on direktiivis ette nähtud makseasutuste tegevusloa nõue. Arvestades, et finantssektoris teenuse osutamiseks peab isikul olema tegevusluba, mille ta saab asukoha finantsjärelevalve asutuselt, ei ole viidatud direktiiviga 2015/2366 kooskõlas olukord, kus makseteenuse osutamine viiakse teise lepinguriiki, kus makseasutusel puudub vastava lepinguriigi finantsjärelevalve asutuse luba selles riigis makseteenuse osutamiseks. Samas ei ole tal võimalik tegevusluba taotleda, kui ta on samal ajal (veel) Eesti registrisse kuuluv äriühing. Direktiivi (EL) 2015/2366 artikli 11 lõike 1 kohaselt antakse tegevusluba üksnes juriidilisele isikule, kes on asutatud selles liikmesriigis (ehk enne tegevusloa taotlemist peaks ta olema sellesse riiki nõ juba ära liikunud).

Kuigi direktiiv (EL) 2019/2121 näeb ette meetmed võlausaldajate kaitseks, ei ole direktiiviga tagatud piisav kliendikaitset juhuks, kui äriühing selles teises liikmesriigis tegevuse jätkamiseks tegevusluba ei saa (teise riiki liikumine ei tähenda automaatselt liidu õigusest tuleneva tegutsemisõiguse üleminekut). ÄS § 491⁸ reguleerib võlausaldajate kaitset, kuid tagatise saamise õigus on vaid võlausaldajal, kelle nõuded on tekkinud enne piiriülese ümberkujundamise projekti avalikustamist, ja nõuete osas, mis ei ole muutunud avalikustamise kuupäevaks sissenõutavaks.

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

MERAS § 63⁵ 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 § 63⁶ pealkirja muutmine. Kuna paragrahvi lisandub ka küberohtudest teavitamine, viiakse paragrahvi pealkiri kooskõlla selle sisuga.

MERAS § 63⁶ täiendamine uute lõigetega 5–8.

Lõige 5. Kuna makseasutustele ja e-raha asutustele hakkab kohalduma DORA määruses sätestatud intsidentidest teatamise kord, on §-i 63⁶ lisatud täpsustus, et DORA määruse kohaldamisalasse kuuluvad makseasutused ja e-raha asutused, sealhulgas erandi alla kuuluvad ja kontoteabe osutajad, lähtuvad operatsiooni- või turvaintsidentidest 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 krediidasutusi, 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:	<ul style="list-style-type: none"> - seab ohtu võrgu- ja infosüsteemide turvalisuse; - avaldab negatiivset mõju andmete kättesaadavusele, autentsusele, terviklusele või konfidentsiaalsusele või finantssektori ettevõtja osutatavatele teenustele. 	<ul style="list-style-type: none"> - 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
	<ul style="list-style-type: none"> - millel on suur negatiivne mõju võrgu- ja infosüsteemidele, mis toetavad finantssektori ettevõtja kriitilise tähtsusega või olulisi funktsioone. 	<ul style="list-style-type: none"> - 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 § 46² lõikes 8 on sätestatud, et Inspeksioon teavitab pärast MERAS § 63⁶ lõikes 1 nimetatud teate saamist viivitamata Euroopa Pangandusjärelevalve Asutust ja Euroopa Keskpanga olulisest operatsiooni- või turvaintsidentist, siis see kohaldub selliste teadete suhtes, mis jäävad MERAS § 63⁶ 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 DORA määruse kohase täitmise üle järelevalve teostamisel kõik nimetatud määruses, MERAS-es ja FIS-is sätestatud õigused.

Nimelt on DORA määruse artikli 50 lõike 1 kohaselt pädevatel asutustel kõik DORA määruse kohaste ülesannete täitmiseks vajalikud järelevalve-, uurimis- ja karistuste määramise volitused ning lõikes 2 on miinimumnimekirja volitustest. 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 kontrollid või uurimisi ning nõuda määruse nõuete rikkumise korral parandus- ja ennetusmeetmete võtmist. Kuna tegemist on miinimumnimekirjaga, siis on FI-l õigus rakendada ka muid MERAS-es ja FIS-is sätestatud õigusi.

Finantsinspeksioonile antakse mh õigus rakendada DORA määruse artikli 50 lõikes 4 sätestatud halduskaristusi ja 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 (kuna liikmesriigi õigusega pole vastavat õigust ette nähtud, siis käesolev meedet ei saa rakendada), ning
- avalike teadaannete väljastamine, mis sisaldavad füüsilise või juriidilise isiku identiteeti ja rikkumise laadi.

Kuna tegemist on jällegi miinimumnimekirjaga, on Finantsinspeksioonil õigus rakendada ka muid MERAS-est ja FIS-ist tulenevaid meetmeid.

Et võetud meetmetel oleks hoiatav mõju laiemale avalikkusele, näeb määrus ette rikkumist puudutavate otsuste avalikustamise. DORA määruse artikli 54 lõike 1 kohaselt avaldavad pädevad asutused oma ametlikel veebisaitidel põhjendamatu viivitusega kõik halduskaristuse määramise otsused, mida ei ole edasi kaevatud pärast seda, kui karistuse saanud isikut on otsusest teavitatud. Lõige 5 näeb samas ette, et kui pädev asutus avaldab halduskaristuse

määramise otsuse, mis on asjaomastele kohtuasutustele edasi kaevatud, lisavad pädevad asutused ühtlasi viivitamata oma ametlikule veebisaidile selle teabe ja hiljem kogu täiendava teabe sellise edasikaebamise tulemuste kohta. Samuti avaldatakse kohtuotsus, millega tühistatakse halduskaristuse määramise otsus.

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.

Kuigi DORA määruse artikkel 54 viitab vaid halduskaristuste avalikustamisele, on FI-l õigus FIS § 54 lõike 5 kohaselt avalikustada lisaks väärteo asjas tehtud lahendile haldusakt või -leping, kui see on vajalik investorite, finantsjärelevalve subjektide klientide või avalikkuse kaitseks või finantsturu õigus- või korrapärase toimimise tagamiseks.

MERAS § 92 muudatused. Seoses MERAS § 24 uue lõikega 4¹ tuleb muuta § 92 lõikeid 1¹ ja 1² nii, et FI-l on viidatud lõigetes sätestatud õigused ja kohustused seoses välisriigis asutatud filiaaliga (kehtiva sõnastus piirdub lepinguriigi filiaaliga).

MERAS uus § 109¹. 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 sätestamisel on lähtutud MERAS-es sätestatud kehtivatest karistusmääradest ja karistuste määramise alustest. Finantssektori karistusnormid on suures osas reguleeritud liidu õiguses, kus reeglina on ette nähtud analoogsed meetmed karistuste rakendamiseks (sh fikseeritud rahaliste suuruste piirmäärad). Makseteenuste ja e-raha teenuste valdkonna EL õigus ei näe ette koosseise konkreetsete karistuste kohta ega rahalisi trahve. Direktiivi 2015/2366 artikli 103 kohaselt tuleb liikmesriigil tagada rikkumiste korral tõhusate, proportsionaalsete ja hoiatavate karistuste rakendamine. Kuna direktiivist 2009/110/EÜ ei tulene otseselt kohustust kohaldada kõrgemaid rahatrahvi määrasid, siis kehtivas MERAS-es kõrgendatud ülemmääraga maksimaalse rahatrahvi kohaldamisel on lähtutud põhimõttest, et direktiivist tulenevate tegevusnõuete rikkumiste puhul kohaldatakse pangandusdirektiivis (2013/36/EL) ette nähtud rahatrahvi määrasid. Seega on ka uue lõike 109¹ sõnastamisel võetud lähenemine, et see oleks kooskõlas MERAS §-dega 109 ja 110.

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, 3–5: 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 § 7¹ lõike 5 muutmine ja lõike 7 kustutamine. 2022. aasta 16. augustil jõustusid KÜTS muudatused, millega ühtlasi tunnistati kehtetuks avaliku teabe seaduse (AvTS) § 43⁹ lõike 1 punktis 4 sätestatud Vabariigi Valitsuse volitusnorm infosüsteemide turvameetmete süsteemi kehtestamiseks, millele EVKS § 7¹ kehtivas lõikes 7 on viidatud. Volitusnormi kustutamist on selgitatud järgmiselt: „Kuna eelnõuga luuakse KÜTS-is võimalus kehtestada E-ITS⁴⁷, siis tuleb ISKE⁴⁸ 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 nõuded.

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

EVKS täiendamine uue §-ga 30² nähakse ette uus paragrahv registripidaja 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 sätestatud 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 § 43¹ 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 § 1² 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.

⁴⁷ Eesti infoturbestandard, https://www.riigiteataja.ee/aktiilisa/1211/2202/2034/MKM_m101_lisa.pdf#

⁴⁸ infosüsteemide kolmeastmelise etalonurbe süsteem

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. Teavitused ja raportid intsidentide kohta tuleb esitada DORA määruse alamaktides kehtestatud vorme kasutades, lähtudes Finantsinspektsiooni kehtestatud andmevahetusvormingust ja teabe edastusviisist (vt tehniliste standardite eelnõu konsultatsioonidokumenti intsidentidest teavitamise kohta).⁴⁹ Nagu käesoleva seletuskirja punkti 2.3.2 alampunktis A kirjeldatud, kasutab finantsasutus nii FI kui ka RIA teavitamisel ühekordset teabedastamise viisi ehk selle kehtestamisel tuleks Finantsinspektsioonil ka selle asjaoluga arvestada.

Intsidentide liigitamise kriteeriumid on ette nähtud DORA määruse artikli 18 lõikes 1, kuid täpsemad kriteeriumid tõsiste intsidentide määramiseks 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 finantsüsteemi, 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 äri vajaduste rahuldamiseks piisavad ressursid, võimed, funktsioonid ja personalikorraldus.

DORA määruse artikli 12 lõike 5 kohaselt peab varutöötluskoht asuma peamisest töötluskohest geograafiliselt eemal, et tagada nende erinev riskiprofiil ja vältida, et varutöötluskohta kahjustab peamisele töötluskohtale mõju avaldanud sündmus. Lisaks peab see varutöötluskoht suutma tagada peamise töötluskohtaga 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.

⁴⁹<https://www.eiopa.europa.eu/system/files/2023-12/JC%202023%2070%20-%20%20CP%20on%20draft%20RTS%20and%20ITS%20on%20major%20incident%20reporting%20under%20DORA.pdf>

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 seaduse⁵⁰ seletuskirjas on selgitatud, et pensioniosakud ei kuulu CSDR-määruse reguleerimisalasse. Seega ei kuulu pensioniregistri pidaja ka DORA määruse kohaldamisalasse. Seetõttu on ka lõikes 7 täpsustatud, et pensioniregistri pidajale ei kohaldata uues paragrahvis sätestatud, sj DORA määruse rakendamise kohustust. Samuti ei välistata neid KÜTS 2. peatüki nõuete rakendamisest.

EVKS § 38 uus lõike 1³ kohaselt teostab FI järelevalvet mh DORA määruses sätestatud nõuete täitmise üle.

EVKS § 39 uus lõige 1¹. Eelnõuga lisatakse paragrahvi uus lõige, milles sätestatakse, et FI-l on DORA määruse kohase täitmise üle järelevalve teostamisel kõik nimetatud määruses, EVKS-is ja FIS-is sätestatud õigused.

Nimelt on DORA määruse artikli 50 lõike 1 kohaselt pädevatel asutustel kõik DORA määruse kohaste ülesannete täitmiseks vajalikud järelevalve-, uurimis- ja karistuste määramise volitused ning lõikes 2 on miinimumnimekiri volitustest. 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 kontrole või uurimisi ning nõuda määruse nõuete rikkumise korral parandus- ja ennetusmeetmete võtmist. Kuna tegemist on miinimumnimekirjaga, siis on FI-l õigus rakendada ka muid MERAS-es ja FISis sätestatud õigusi.

Finantsinspeksioonile antakse mh õigus rakendada DORA määruse artikli 50 lõikes 4 sätestatud halduskaristusi ja 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 (kuna liikmesriigi õigusega pole vastavat õigust ette nähtud, siis käesolev meedet ei saa rakendada), ning
- avalike teadaannete väljastamine, mis sisaldavad füüsilise või juriidilise isiku identiteeti ja rikkumise laadi.

Kuna tegemist on jällegi miinimumnimekirjaga, on Finantsinspeksioonil õigus rakendada ka muid EVKS-ist ja FIS-ist tulenevaid meetmeid.

EVKS § 39 uus lõige 4¹. FI peab avalikustama DORA määruse rikkumisega seoses võetud meetmete alusel tehtud otsuse kohta teate oma veebilehel nagu on sätestatud artiklis 54.

Et võetud meetmetel oleks hoiatav mõju laiemale avalikkusele, näeb määrus ette rikkumist puudutavate otsuste avalikustamise. DORA määruse artikli 54 lõike 1 kohaselt avaldavad pädevad asutused oma ametlikel veebisaitidel põhjendamatu viivitusega kõik halduskaristuse

⁵⁰

<https://www.riigikogu.ee/tegevus/elnoud/elnou/cec5e4d6-98a5-4016-965a-c151c9e94354/eesti-vaartpaberite-keskregistri-seaduse-muutmise-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus>

määramise otsused, mida ei ole edasi kaevatud pärast seda, kui karistuse saanud isikut on otsusest teavitatud. Lõige 5 näeb samas ette, et kui pädev asutus avaldab halduskaristuse määramise otsuse, mis on asjaomastele kohtuasutustele edasi kaevatud, lisavad pädevad asutused ühtlasi viivitamata oma ametlikule veebisaidile selle teabe ja hiljem kogu täiendava teabe sellise edasikaebamise tulemuste kohta. Samuti avaldatakse kohtuotsus, millega tühistatakse halduskaristuse määramise otsus.

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.

Kuigi DORA määruse artikkel 54 viitab vaid halduskaristuste avalikustamisele, on määruse (EL) nr 909/2014 (CSDR) artiklis 62 sätestatud, et viidatud määruse rikkumise eest avalikustatakse otsus nii halduskaristuse kui ka muu haldusmeetme kohta. Kuna DORA nõuded integreeritakse viidatud määrusesse (vt DORA määruse artiklit 61), on pädeval asutusel alus avalikustada lisaks halduskaristustele ka muud meetmed (nt ettekirjutus), kui rikutakse DORA nõudeid.

3.10. Eelnõu § 10. Väärtpaberituruse 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 237⁹⁰ ehk karistusi DORA määruse nõuete rikkumise eest kohaldatakse ka viidatud ühisrahastusteenuse osutajatele.

VpTS § 10¹ 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 § 70¹ 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 tunnistanud 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 ära kirja, kui põhikirja või ühingulepingu registrile esitamine on nõutav ka ühingu asukohamaal.

VpTS § 81¹ täiendamine uue lõikega 4¹. Paragrahv reguleerib investeerimisühingu üldisi organisatsiooninõudeid. Muudatusega nähakse ette investeerimisühingu kohustus rakendada mh DORA määrust.

VpTS § 82⁶ 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 kehtiva sõnastuse kohaselt peab olulise tööülesande või tegevuse edasiandmisel olema täidetud viidatud delegeeritud määruses ja VpTS-is 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 § 82¹⁵ 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 väärtpäberituru korra- või õiguspärasust toimimist. Sama lõike teises lauses on sätestatud, et investeerimisühing järgib selliste meetmete rakendamisel muu hulgas komisjoni delegeeritud määruses (EL) nr 2017/589 sätestatud. Muudatusega lisatakse viide lisaks DORA määrusele.

VpTS § 82¹⁵ 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 varurajatist.

VpTS uus § 82¹⁸. 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. Teavitused ja raportid intsidentide kohta tuleb esitada DORA määruse alamaktides kehtestatud vorme kasutades, lähtudes Finantsinspektsiooni kehtestatud andmevahetusvormingust ja teabe edastusviisist (vt tehniliste standardite eelnõu konsultatsioonidokumenti intsidentidest

teavitamise kohta).⁵¹ Nagu käesoleva seletuskirja punkti 2.3.2 alampunktis A kirjeldatud, kasutab finantsasutus nii FI kui ka RIA teavitamisel ühekordset teabeedastamise viisi ehk selle kehtestamisel tuleks Finantsinspektsioonil ka selle asjaoluga arvestada.

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 finantsüsteemi, 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. Direktiivi (EL) 2019/2121 põhjenduspunkti 57 kohaselt ei tohiks viidatud direktiiv mõjutada liidu õiguse kohaldamist, mis reguleerib krediitvahendustevõtjaid ja teisi finantstevõtjaid, ega vastavalt kõnealusele liidu õigusele kehtestatud liikmesriigi õigusnormide kohaldamist. Investeerimisühingute tegevust reguleeriva direktiivi 2014/65/EL põhjenduspunktis 3 on osutatud, et finantsturgudel on tegutsema asunud rohkem investoreid ja neile pakutakse veelgi keerukamat ulatuslikku teenuste ja instrumentide valikut, mistõttu peaks liidu õigusraamistik hõlmama kogu investoritele suunatud tegevust. Selleks on vaja näha ette ühtlustamise tase, mida on vaja investoritele kõrgetasemelise kaitse pakkumiseks ja selleks, et võimaldada investeerimisühingutel osutada päritoluriigi järelevalve all teenuseid kogu liidus, mis on siseturg. Selle tagamise üheks meetmeks on direktiivis ette nähtud investeerimisühingu tegevusloa nõue.

Arvestades, et finantssektoris teenuse osutamiseks peab isikul olema tegevusluba, mille ta saab asukoha finantsjärelevalve asutuselt, ei ole viidatud direktiiviga 2014/65/EL kooskõlas olukord, kus investeerimisühingu tegevus viiakse teise lepinguriiki, kus investeerimisühingul puudub vastava lepinguriigi finantsjärelevalve asutuse luba selles riigis teenuse osutamiseks. Samas ei ole tal võimalik tegevusluba taotleda, kui ta on samal ajal (veel) Eesti registrisse kuuluv äriühing. Kuigi direktiiv (EL) 2019/2121 näeb ette meetmed võlausaldajate kaitseks, ei ole direktiiviga tagatud piisav investorkaitset juhuks, kui äriühing selles teises liikmesriigis tegevuse jätkamiseks tegevusluba ei saa (teise riiki liikumine ei tähenda automaatselt liidu õigusest tuleneva tegutsemisõiguse üleminekut). Samuti ei ole reguleeritud, mis saab kliendiportfellidest perioodil, kui ühing alles taotleb uues liikmesriigis tegevusluba teenuse osutamise jätkamiseks. ÄS § 491⁸ reguleerib võlausaldajate kaitset, kuid tagatise saamise õigus on vaid võlausaldajal, kelle nõuded on tekkinud enne piiriülese ümberkujundamise projekti avalikustamist, ja nõuete osas, mis ei ole muutunud avalikustamise kuupäevaks sissenõutavaks.

VpTS § 119¹⁷ 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 sätestatud.

⁵¹<https://www.eiopa.europa.eu/system/files/2023-12/JC%202023%2070%20-%20CP%20on%20draft%20RTS%20and%20ITS%20on%20major%20incident%20reporting%20under%20DORA.pdf>

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

VpTS § 124⁶ lõigete 1 ja 3 muutmine. Paragrahv 124⁶ 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 sätestatud.

VpTS § 124⁶ 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 § 124⁶ lõikes 3. Kuna samas sättes on defineeritud kauplemissüsteem, on eelnõus otsustatud seda sätet mitte kustutada, vaid lisada sinna viide DORA määrusele.

VpTS § 124⁶ uus lõige 9. NIS2 direktiivi subjektide hulka kuuluvad mh Euroopa Parlamendi ja nõukogu direktiivi 2014/65/EL artikli 4 punktis 24 määratletud kauplemiskohtade korraldajad ning Euroopa Parlamendi ja nõukogu määruse (EL) nr 648/2012 artikli 2 punktis 1 määratletud kesksed vastaspoolad (vt NIS2 direktiivi lisa I punkti 4). Kuna DORA määruse on NIS2 direktiivi suhtes *lex specialis* ehk NIS2 direktiivi sätete asemel tuleks kohaldada samaväärseid DORA määruse sätteid, on selguse huvides välja toodud, et korraldaja suhtes ei kohaldata KÜTS 2. peatükis sätestatud küberturvalisuse nõudeid.

VpTS § 125¹ 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 taasteplaani.

VpTS § 125² 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 sätestatud.

VpTS uus § 125³. 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. Teavitused ja raportid intsidentide kohta tuleb esitada DORA määruse alamaktides kehtestatud vorme kasutades, lähtudes Finantsinspeksiooni kehtestatud andmevahetusvormingust ja teabe edastusviisist (vt tehniliste standardite eelnõu konsultatsioonidokumenti intsidentidest teavitamise kohta).⁵² Nagu käesoleva seletuskirja punkti 2.3.2 alampunktis A kirjeldatud, kasutab finantsasutus nii FI kui ka RIA teavitamisel ühekordset teabeedastamise viisi ehk selle kehtestamisel tuleks Finantsinspeksioonil ka selle asjaoluga arvestada.

⁵²<https://www.eiopa.europa.eu/system/files/2023-12/JC%202023%2070%20-%20%20CP%20on%20draft%20RTS%20and%20ITS%20on%20major%20incident%20reporting%20under%20DORA.pdf>

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 § 163¹ lõike 7 muutmine. Sättesse lisatakse viide uuele VpTS §-le 125³. 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. Kuna § 230 lõike 1 teine lause viitab rikkumise korral ainult VpTS ja FIS meetmete rakendamisele, täpsustatakse lõike 7 esimeses lauses, et FI-l on mh õigus rakendada DORA määruses sätestatud meetmeid.

FI peab avalikustama DORA määruse rikkumise korral võetud meetmete alusel tehtud otsuse kohta teate oma veebilehel nagu on sätestatud artiklis 54.

Et võetud meetmetel oleks hoiatav mõju laiemale avalikkusele, näeb määrus ette rikkumist puudutavate otsuste avalikustamise. DORA määruse artikli 54 lõike 1 kohaselt avaldavad pädevad asutused oma ametlikel veebisaitidel põhjendamatu viivitusega kõik halduskaristuse määramise otsused, mida ei ole edasi kaevatud pärast seda, kui karistuse saanud isikut on otsusest teavitatud. Lõige 5 näeb samas ette, et kui pädev asutus avaldab halduskaristuse määramise otsuse, mis on asjaomastele kohtuasutustele edasi kaevatud, lisavad pädevad asutused ühtlasi viivitamata oma ametlikule veebisaidile selle teabe ja hiljem kogu täiendava teabe sellise edasikaebamise tulemuste kohta. Samuti avaldatakse kohtuotsus, millega tühistatakse halduskaristuse määramise otsus.

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 väärtemenetlust, 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.

Kuigi DORA määruse artikkel 54 viitab vaid halduskaristuste avalikustamisele, on direktiivi 2014/65/EL artiklis 71 sätestatud, et liikmesriigid tagavad, et pädevad asutused avaldavad oma ametlikul veebisaidil kõik otsused halduskaristuste või muude meetmete kohta, mis on mõistetud või võetud määruse (EL) nr 600/2014 või käesoleva direktiivi (2014/65/EL) rakendamiseks vastu võetud siseriiklike sätete rikkumise eest. VpTS § 230 lõike 4¹ kohaselt avalikustab FI oma veebilehel seaduse 3., 31. ja 4. osas sätestatud kohustuse rikkumisega seoses

tehtud väärtetasja lahendi või haldusakti viivitamata pärast selle teatavaks tegemist ehk vastav sätte anna aluse ka muude meetmete (nt ettekirjutus) avalikustamiseks, kui rikutakse DORA nõudeid.

VpTS uus § 237⁹⁰. 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 väärteto tulemusel teenitud kasule või ära hoitud kahjule vastavas summas ning juriidilise isiku korral karistatakse rahatrahviga kuni 5 000 000 eurot või kuni kahekordse väärteto tulemusel teenitud kasule või ära hoitud kahjule vastavas summas või kuni kümme protsenti juriidilise isiku või tema konsolideerimisgrupi konsolideeritud käibest.

Uue paragrahvi sätestamisel on lähtutud VpTS-is sätestatud kehtivatest karistusmääradest ja karistuste määramise alustest. Finantssektori karistusnormid on suures osas reguleeritud liidu õiguses, kus reeglina on ette nähtud analoogsed meetmed karistuste rakendamiseks (sh fikseeritud rahaliste suuruste piirmäärad). Kuna DORA määruse nõuded integreeritakse DORA direktiiviga vastavatesse finantssektori õigusaktidesse (investeeringisühingute ja korraldajate puhul direktiivi 2014/65/EL), on ka eelnõu puhul võetud lähenemine, et DORA nõuete rikkumise eest ette nähtud karistused oleksid kooskõlas vastavates liidu õigusaktides ette nähtud karistussätetega. VpTS uue paragrahvi puhul on võetud aluseks direktiivi 2014/65/EL artikli 70 lõike 3 punkti a alapunktid iv, v, xxvii ja xxviii ning lõike 6 punktid f–g. DORA direktiivi kohaselt muudetakse 2014/65/EL direktiivi artikleid 16 ja 17 ning 47 ja 48 nii, et sinna lisatakse viited DORA nõuete rakendamisele. Kuna direktiivi 2014/65/EL artikli 70 lõike 3 punkti a alapunktid viitavad nende artiklite rikkumistele, hõlmab see ühtlasi DORA nõuete rikkumist.

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, 3–5: 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 § 237⁸⁹ ja § 262² kehtetuks tunnistamine ning uus § 262³. Muudatus on normitehniline, menetluse paragrahvi asukoht muutub. Samuti tõstetakse menetluse paragrahvi väärtegade aegustähtaeg, mistõttu tunnistatakse § 262² kehtetuks. Väärtegade nn üldine aegumise tähtaeg on kaks aastat. KarS § 81 lõige 3 võimaldab väärtegade kaheaastase aegumistähtaja asemel ette näha ka viieaastase aegumistähtaja. Finantsinspeksioon on korduvalt tähelepanu juhtinud, et üldine aegumise tähtaeg ei ole finantsvaldkonnas toimepandud väärtegade keerukuse tõttu menetluse läbiviimiseks piisav.

Finantssektori väärtegade kolmeaastased aegumistähtajad nähti ette finantsvaldkonna väärtekaristuste reformi raames. Paralleelselt menetleti JuMi vastutusvaldkonda kuuluvat karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadust (Euroopa Liidu õigusest tulenevad rahatrahvid), mille seletuskirjas on selgitatud, et „väljatöötamiskavatsuse kooskõlastamisel avaldati arvamust, et kõrgema rahatrahvi

ülemääraga karistatavate väärtegade korral tuleks sätestada senisest pikem aegumistähtaeg. Eelnõu koostamisel leiti algselt, et kuna kehtiv õigus võimaldab teatud väärtegade korral sätestada kaheaastase aegumistähtaja asemel kolmeaastase aegumistähtaja (KarS § 81 lg 3) ning suurema ebaõigussisuga teise astme kuritegu aegub viie aastaga (KarS § 81 lg 1 p 2), ei ole praegu erisuse loomine vajalik. Sellegipoolest leiti ka eelnõu kooskõlastamisel esitatud arvamustes jätkuvalt, et väärtegade üldine aegumistähtaeg ei võimalda finants- ja andmekaitse valdkonnas väärtemenetlusi tõhusalt läbi viia, arvestades nendes valdkondades toime pandavate väärtegade keerukust“. Teise lugemise seletuskirjas on lisaks, et „esimese lugemise läbinud eelnõus ei nähtud ette väärtegade aegumistähtaja pikendamist, vaid sätestati täiendavad aegumise katkemise alused. Arvestades siiski teatud valdkondade eripära, võib senisest suuremate trahvide korral olla põhjendatud ka pikemate aegumistähtaegade sätestamine. Nii näiteks on EL määruse (EU) 468/2014 artikli 130 kohaselt Euroopa Keskpanga poolt kohaldatavate trahvide korral aegumistähtajaks 5 aastat. Kui krediidiastutus ei allu Euroopa Keskpanga järelevalvele, oleks Eestis sama rikkumise korral aegumistähtaeg põhjendamatult lühem. Kehtiv KarS § 81 lg 3 näeb ette, et üldreeglina on väärtete aegumistähtaeg 2 aastat ning seaduses sätestatud juhtudel võib ette näha kolmeaastase aegumistähtaja. Ettepaneku kohaselt jääks KarS § 81 lg 3 üldreegliks 2 aastat, kuid seaduses võib ette näha ka kuni 5-aastase aegumistähtaja (so kolme-, nelja- või viieaastase aegumistähtaja). Arvestades siiski, et 5-aastane aegumistähtaeg on ka teise astme kuriteo aegumistähtajaks, peaks nii pikk aegumistähtaeg väärtegade korral olema siiski erandlik.“.

Finantsvaldkonnas võib olla tegemist väga keeruliste kaasustega, mis on tavaliselt nn peitsüüteod (nagu näiteks ka maksustamise valdkonna süüteod), s.t. rikkumise toimepanemise asjaolud ei ole kergelt märgatavad, kannatanud ei ole või tema isik ei ole teada ja süüteo toimepannud isik teeb kõik endast oleneva, et järelevalveasutus ei avastaks rikkumist.

Seaduse normitehniline märkuse. Muudatusega lisatakse viide DORA direktiivile.

Eelnõu § 11. Seaduse jõustumine.

DORA nõuete rakendamiseks vajalikud seadusemuudatused jõustuvad 17. jaanuaril 2025. Kindlustussummade muutmise määruse muudatused jõustuvad 2024. aasta 9. oktoobril. Vastav jõustumiskuupäev on ette nähtud kindlustussummade muutmise määrus artiklis 2. Ülejäänud muudatused jõustuvad 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 usaldusväarsust, 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 1 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	<p>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. Osaliselt on määrusega kehtestatavad nõuded juba kaetud erinevate standardite, seaduste ja suunistega: ISO/IEC 27000 standardipere 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 <i>Cyber Resilience Oversight Expectations</i>. Seega kõik DORA nõuded ei ole ettevõtjate jaoks täiesti uued, kuid DORA eesmärk on ühtlustada ja spetsifitseerida IKT-riskidega seotud seniseid nõuded, mistõttu sõltub kaasnev mõju mh sellest, mis ulatuses ja tasemel on ettevõtjad seni tegelenud IKT-riskide juhtimise ja küberturvalisuse tagamisega ehk milline on nende hetkeseis DORA nõuetele vastamisel ja millised puudused tuleb nõuetele vastavuse tagamiseks kõrvaldada. See on tase on ettevõtjatel erinev, sõltudes ka vastavast finantssektorist.</p> <p>Kuigi suuremad ja keerukamad finantsasutused juba omavad keerulisi IKT-süsteeme ja protseduure, tähendab ka nende läbivaatamine ja DORA nõuetega kooskõlla viimine halduskoormuse tõusu.</p> <p>Võib väita, et digitaalse tegevuskerksuse nõuete rakendamiseks peavad finantsasutused teatud ümberkorraldusi tegema (nt juhtimisstruktuuri tõhustamine), mis eeldab täiendavate rahaliste vahendite kaasamist. Samas sõltub see taas finantsasutusest ja tema tegevusprofiilist, kas</p>

juhtimiskorralduses on vaja teha muudatusi seoses uute isikute tööle värbamisega. Lisaks on määrusega 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. Viidatud programmid ja koolitused tähendavad jällegi kulusid ettevõtjale. Kuna küberturvalisuse tagamine on ettevõtjasisene pidev protsess, siis on ka sellega kaasnevad kulud pidevad. Samas on DORA üheks oluliseks põhimõtteks, et finantsasutused peaksid IKT-riski juhtimise raamistiku rakendamiseks ressurside ja suutlikkuse jaotamisel võtma oma IKT-ga seotud vajaduste puhul igakülgset arvesse oma suurust ja üldist riskiprofiili ning oma teenuste, tegevuse ja toimingute laadi, ulatust ja keerukust. Seega ka kulud peaks olema proportsioonilise 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 aastaraamatus⁵³ 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 (süvatestimine) kohalduvad olulistele ja kübervõimekatele teenuseosutajatele (näiteks suured, süsteemselt olulised ja IKT seisukohast küpsed krediidasutused, börsid, väärtipaberite keskodepositooriumid ja kesksed vastaspooled). Seega võib väita, et süvatestide tegemisega kaasnev halduskoormuse tõus ja rahaliste kulude suurenemine mõjutab siiski väikest, aga olulist osa finantssektorist. Kuna testimist tuleb läbi viia iga kolme aasta tagant, avaldub viidatud mõju suures osas iga kolme aasta tagant (samas võib pädev asutus nõuda põhjendatud juhul ka sagedamast testimist ning sellisel juhul avaldub mõju sagedamini).

Kuna ohuteabel põhineval läbistustestimisel tuleb üldjuhul kasutada välistestijaid/Red Team'i (sisetestijad on lubatud teatud tingimustel ja vaid pädeva asutuse nõusolekul), siis see tähendab ettevõtja jaoks samuti

⁵³https://www.fi.ee/sites/default/files/2023-04/Finantsinspektsiooni%20aastaraamat%202022_0.pdf

	<p>märkimisväärseid kulusid. Kulud võivad varieeruda sõltuvalt ettevõtja suurusest, tegevusvaldkonnast, turvameetmete tasemest, keerukusest, testimise ulatusest jne, jäädes keskmiselt 40 000 euro kanti. Sisemiste testijate kasutamisel ei ole kulud eelduslikult nii suured, kuid ettevõtja peab tagama sisemiste testijate koolitamise. Kuigi kulud võivad olla märkimisväärsed, on see oluline investeering ettevõtte turvalisuse tagamiseks ja võimalike kahjude, sealhulgas mainekahju, ennetamiseks. Andmelekked võivad ettevõtjale maksta minna miljoneid eurosid.</p> <p>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 (näiteks võib finantsasutus sõlmida lepingu IKT teenuseosutajaga, kes vastab asjakohastele infoturbestandarditele) ja finantsasutus peab leidma partneri, kellega seotud kulud võivad olla suuremad kui seni oli arvestatud.</p> <p>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.</p> <p>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.</p>
<p>Ebasoovitavate mõjude avaldumise risk</p>	<p>Ebasoovitavate mõjude avaldumise 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.</p> <p>Seega jääb alati ülesse risk, et vaatamata küberkerksuse nõuete rakendamisele, on küberründajad ettevõtjatest kaks sammu ees.</p> <p>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.</p>

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 usaldusväarsust 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 klientidele 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 järelevalvamise alla, teevad ESA-d.

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

Mõju ulatus ja avaldumise sagedus	ESA-d hakkavad teostama Euroopa-ülest järelevaatamist kriitilise tähtsusega ITK teenuseosutajate üle ning sellega kaasnevaid kulusid rahastatakse täielikult kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatele kehtestatud tasudest. Seega tähendab uus regulatsioon rahalisi kulusid ainuüksi tasude näol.
Ebasoovitavate mõjude avaldumise risk	Kui teenuseosutaja ei ole teavitanud juhtivat järelevalveasutust, kas ta järgib talle tehtud soovitusi või mitte või kui teenuseosutaja selgitus ei ole piisav selle kohta, miks ta ei järgi soovitusi, 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 riigiasutuste ja kohaliku omavalitsuse korraldusele

Sihtrühm: FI ja RIA.

Mõju riigiasutuste ja kohaliku omavalitsuse korraldusele	
Mõju ulatus ja avaldumise sagedus	<p>Finantsinspeksioon</p> <p>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.</p> <p>Kuigi FI valmisolek teostada DORA määruse nõuete üle järelevalvet on juba käesoleval hetkel väga hea, on Finantsinspeksioon alustanud kübervaldkonna erialase taseme tõstmisega ja ekspertide kaasamisega (täiendavad töökohad ja erialased koolitused) ning vastavate kulutustega on 2024. a eelarve koostamisel juba ka arvestanud. Finantsinspeksioon kavandab juurde luua 12 täiendavat töökohta, kuid need seonduvad lisaks digitaalse tegevuskerksuse nõuete järelevalvele ka inkasso valdkonna järelevalve mehitamise ja uute ülesannetega seoses kriisilahendusega.</p> <p>Finantsinspeksiooni 2022. aasta aastaraamatus on kirjas, et „Finantsinspeksioon hindab oma järelevalvetegevuse käigus muu hulgas pankade IT-organisatsiooni, IT-struktuuri ja haldust, talitluspidevust, arendustöid, turvalisust ja küberriskide juhtimist tervikuna. Finantsinspeksioon analüüsib regulaarse aruandluse põhjal kõiki olulisi intsidente, vajadusel küsib pankadelt tegevuskavasid ning jälgib, et rakendataks meetmeid, mis aitavad tulevikus sarnaste intsidentide kordumist vältida. Inspeksioon koostab valdkonnaüleseid IT- ja küberriskianalüüsi, mille põhjal tuvastab suure IT-riskiga finantssektori osad. Suurte IT-riskidega pangad peavad välja töötama tegevuskavad, mida Finantsinspeksioon jälgib eriaruandluse korras. Lähtuvalt riskidest analüüsib inspeksioon detailsemaid teemasid – aastal 2022 oli fookus pankade küberriskide haldusel ja maandamisel ning IT turvatestimiste protsessi toimimisel.“</p>

	<p>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.</p> <p>ESA-de DORA määruse rakendamiseks vajalike IKT-süsteemide arendamist rahastatakse esialgu liidu ja riiklike pädevate asutuste osamaksetest (hiljem kaetakse püsikulud kriitiliste IKT-teenuseosutajate enda tasudest). Kuna ESA-d alles koostavad vastavaid eelarveid, ei ole hetkel teada, kas või kui palju see FI osamakse suurust võib mõjutada.</p> <p>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 ressursiga.</p> <p>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.</p>
Ebasoovitavate mõjude avaldumise risk	Ebasoovitavate mõjude avaldumise riski ei tuvastatud.
Mõju olulisus	Mõju võib pidada keskmiseks.

Seadus ei mõjuta kohalike omavalitsuste korraldust.

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.

Eelnõu koostamise käigus ei ole tehtud andmekaitse mõjuhindangut, kuna eelnõu alusel ei töödeldaks GDPR artiklist 35 tulenevaid isikuandmeid, millest võiks tekkida suur oht isikute õigustele ja vabadustele.

6.6. Mõjude kokkuvõte

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

Halduskoormuse klientidele. Eelnõu ei mõjuta finantsteenuste klientide halduskoormust.

Halduskoormus avalikule sektorile. Avaliku sektori halduskoormus võib suureneeda, 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. RIA koostöö FI-ga ja tehnilise nõu andmine võib tähendada riigieelarve kulude suurenemist.

8. Rakendusaktid

Eelnõuga ei kehtestata uusi rakendusakte. Samuti ei ole vaja muuta ja tunnistada kehtetuks kehtivaid 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. Juhendite koostamine ja ajakohastamine kuulub FI pädevusse.

9. Seaduse jõustumine

Seadus jõustub osaliselt 17. jaanuaril 2025. a. Jõustumise tähtaeg on seotud DORA nõuete rakendamise kuupäevaga, milleks on 17. jaanuar 2025. a (vt DORA määruse artikkel 64).

Komisjoni kindlustussummade muutmise määrusest tulenevad muudatused jõustuvad 2024. aasta 9. oktoobril (kindlustussummade määruse artikkel 2). Kuna uutele kindlustussummadele üleminekuks on ette nähtud vaid kuus kuud, on vastavad muudatused lisatud käesolevasse eelnõusse, et asjakohased kindlustusvahendajad oleksid aegsasti teadlikud muudetud summadest.

Muud muudatused, mis ei ole seotud DORA direktiivi ülevõtmise ja kindlustussummade muutmisega, jõustuvad üldkorras. Muudatus õigusnormide kohaldamiseks ei ole vajalik ette näha ülemineku perioodi, kuna muudatused on osaliselt normitehnilised.

10. Eelnõu kooskõlastamine ja huvirühmade kaasamine

Eelnõu esitati 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.

Märkustega tagasiside saadi Justiitsministeeriumist, Majandus- ja Kommunikatsiooniministeeriumist, Finantsinspektsioonist, Riigikantseleist, MTÜ FinanceEstoniast, Eesti Pangaliidult, Eesti Kindlustusseltside Liidust ja Eesti Kaubandus-Tööstuskojalt (vt märkuste tabelit lisa 2).

Heili Tõnisson
 Valitsuse nõunik

LISA 1. 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 riigisisised 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	KindlITS § 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 riigisisised õigusaktid	Kommentaar
Art 2 lg 4	Valikuline	HLÜS § 2 ¹	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, ESMA-t, EBA-t ja EIOPA-t 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, KindITS 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 , KindITS § 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	