Võlaõigusseaduse ja sellega seonduvalt teiste seaduste muutmise seaduse (finantspettuste ennetamine ja tõkestamine) eelnõu seletuskiri

1. Sissejuhatus

1.1. Sisukokkuvõte

Eelnõu eesmärk on tõhustada finantspettuste ennetamise ja tõkestamise meetmeid. Viimastel aastatel on finantspettuste arv ja keerukus märkimisväärselt kasvanud[1]. Pettuste toimepanemiseks kasutatakse näiteks erinevaid digitaalseid kanaleid ja tehnilisi vahendeid ning identiteedivargust ja sotsiaalset manipuleerimist, mille abil petetakse isikutelt raha välja. Finantspettused on kiiresti kasvav probleem – mullu kaotasid Eesti inimesed petturitele ligi 29 miljonit eurot, peaaegu kaks korda rohkem kui aasta varem. Enamik pettusi algab telekommunikatsioonikanalite kaudu ja lõpeb pangamaksega, mistõttu on tõhus ennetus võimalik vaid riigi ja erasektori tihedas koostöös.

Eelnõu tugevdab makseteenuse kasutajate kaitset olukorras, kus makse tegemisel esineb pettusekahtlus, ning parandab makseteenuse pakkujate võimalusi finantspettusi ennetada ja tõkestada. Praktikas on pettuste puhul küll makse tehniliselt kinnitatud, kuid hiljem ilmneb, et maksja ei ole teinud makset oma tegeliku ja vaba tahte alusel, vaid teda on selleks eksitatud. Kehtiv õigus ei anna selliste olukordade lahendamiseks piisavaid võimalusi. Eelnõu loob selgema õigusraamistiku ja tugevdab pankade õigust põhjendatud pettuse kahtluse korral makseid ajutiselt peatada või makse täitmisest keelduda. Eelnõu annab ka krediidiasutustele ja makseasutustele ja e-raha asutustele (edaspidi koos *makseteenuse pakkujad*) selge õigusliku aluse pettusekahtlusega seotud info vahetamiseks teiste krediidiasutuste, makseasutuuste ja e-raha asutuste, Politsei- ja Piirivalveameti (edaspidi *PPA*) ning Riigi Infosüsteemi Ameti (edaspidi *RIA*) küberintsidentide käsitlemise osakonna CERT-EE-ga (edaspidi *CERT*).

Esiteks, eelnõuga muudetakse võlaõigusseaduse (edaspidi *VÕS*) regulatsiooni, mis puudutab maksejuhise täitmisest keeldumist ehk olukorda, kus isik soovib teha maksetehingut, kuid makseteenuse pakkuja (pank või makseasutus) saab keelduda maksetehingu täitmisest. Kehtivas õiguses puudub makseteenuse pakkujal selge õiguslik alus keelduda maksejuhise täitmisest juhul, kui on põhjendatud kahtlus, et maksetehingu täitmiseks antud nõusolek on saadud andmete väärkasutamise, pettuse või maksja manipuleerimise teel. Praktikas võib see tähendada olukorda, kus makseteenuse pakkuja näeb, et makse on küll kinnitatud nõutud autentimisvahenditega, kuid esineb põhjendatud kahtlus, et need vahendid on saadud või on neid kasutatud pettuse teel. Näiteks võib isik olla petuskeemi käigus eksitatud kinnitama makset, uskudes, et ta suhtleb pangaga, kuigi tegelikult suunab teda makset tegema pettur. Kuigi makse on tehniliselt kinnitatud kliendi autentimisvahendiga, on nõusolek sellisel juhul antud pettuse teel isiku eksitusse viimisega.

[1] Vt Eesti Panga koostatud ülevaadet: https://haldus.eestipank.ee/sites/default/files/2025-12/ep_maksepettuste-ulevaade-2025_0.pdf

Teiseks, eelnõuga muudetakse krediidiasutuste seadust (edaspidi *KAS*), millega antakse krediidiasutustele õigus jagada vajalikku teavet pettuste avastamiseks ja väljaselgitamiseks. Seda juhul kui krediidiasutusel on objektiivselt põhjendatud kahtlus, et klient või maksetehing võib olla seotud pettusega. Eelnimetatud teave võib mh kvalifitseeruda ka pangasaladuseks. **Krediidiasutusel saab olema õigus omal initsiatiivil jagada vajalikku teavet teiste krediidiasutustega, makseasutuste ja e-raha asutustega, PPA-ga ning RIA-ga.** Kehtivas õiguses selline õigus puudub ning see on osutunud probleemiks pettuste avastamisel ja väljaselgitamisel. Praktikas tähendab see, et näiteks olukordades, kus krediidiasutusel on kahtlus, et konkreetne maksekonto (lihtsustatult arvelduskonto) on seotud pettuste toimepanemisega, siis seda teadmist teiste krediidiasutustega jagada ei tohi. Sellise õiguse puudumine on takistuseks tõhusamalt ennetada pettuste toimepanemist. Samuti antakse krediidiasutusele õigus avaldada andmeid e-identimise ja e-tehingute usaldusteenuste seaduse tähenduses e-allkirjastamist võimaldavale usaldusteenuse osutajale. Krediidiasutus ise ei halda usaldusteenuse osutaja allkirjastamiskeskkonda ega selle tehnilisi logisid. Andmete avaldamise eesmärk on võimaldada usaldusteenuse osutajal kontrollida, kas pettuslik tehing seostub näiteks sama kasutaja või sama seadmega.

Kolmandaks, eelnõuga muudetakse makseasutuste ja e-raha asutuste seadust (edaspidi *MERAS*) ja antakse makseasutustele ja e-raha asutustele õigus avaldada andmeid ja teavet teisele makseasutusele ja e-raha asutusele, krediidiasutusele, PPA-le ning RIA-le maksepettuste avastamiseks ja väljaselgitamiseks KAS §-is 89^4 sätestatud tingimustel. Kuna makseteenuseid osutavad ka makseasutused ja e-raha asutused, antakse ka neile krediidiasutusega samasugune õigus andmeid avaldada. Vastasel juhul jääks osa teenusepakkujaid pettuste ennetustegevusest väljapoole puuduva info tõttu. Andmete avaldamise eesmärk ja koosseis on sama nagu krediidiasutustel.

Kavandatavad muudatused võimaldavad makseteenuse pakkujatel pettusekahtluse korral kiiremini sekkuda ning teha omavahel, samuti PPA ja RIA-ga, koostööd, aidates seeläbi vähendada pettustega tekitatud kahju ja suurendada finantssüsteemi turvalisust. Muudatused ei too kaasa täiendavat halduskoormust makseteenuse pakkujatele ega avaliku sektori asutustele, vaid aitavad pettuste ennetamist ja tõkestamist paremini korraldada.

1.2 Eelnõu ettevalmistaja

Eelnõu ja seletuskirja on koostanud Rahandusministeeriumi finantsteenuste poliitika osakonna nõunik Jarmo Lilium (e-post: jarmo.lilium@fin.ee). Eelnõu juriidilist kvaliteeti kontrollis õigusosakonna nõunik Marge Kaskpeit (e-post: marge.kaskpeit@fin.ee). Eelnõu on keeleliselt toimetanud Rahandusministeeriumi personali- ja õigusosakonna keeletoimetaja Heleri Piip (e-post: heleri.piip@fin.ee).

1.3 Märkused

Eelnõuga muudetakse:

- Krediidiasutuste seadust redaktsioonis RT I, 13.02.2026, 7;
- Võlaõigusseadust redaktsioonis RT I, 11.11.2025, 16;

- Makseasutuste ja e-raha asutuste seadust redaktsioonis RT I, 13.02.2026, 9.

Eelnõu on seotud järgmiste Euroopa Liidu õigusaktiga:

- Euroopa Parlamendi ja nõukogu direktiiv (EL) 2015/2366 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 (ELT L 337, 23.12.2015, lk 35–127)[2] (edaspidi *makseteenuste direktiiv*);
- Euroopa Parlamendi ja nõukogu määrus (EL) 2024/886, millega muudetakse määrusi (EL) nr 260/2012 ja (EL) 2021/1230 ning direktiive 98/26/EÜ ja (EL) 2015/2366 eurodes välkkreeditkorralduste osas (ELT L, 19.3.2024.)[3] (edaspidi *välkmaksete määrus*).

Eelnõu ei ole seotud muu menetluses oleva eelnõuga, kuid on seotud Vabariigi Valitsuse 2025–2027 tegevusprogrammiga. Koalitsioonileppe punkti 308 kohaselt on ette nähtud, et koostöös Eesti Panga, erasektori ja teiste asutustega töötakse välja finantspettuste tõkestamise tegevuskava ja tehakse selle põhjal vajalikud muudatused seadusandluses.[4]

Vastavalt Eesti Vabariigi põhiseaduse (edaspidi *PS*) §-le 73 võetakse eelnõu seadusena vastu Riigikogu poolthäälte enamusega, kui PS ei näe ette teisiti. Eelnõus ei ole sätteid, mis puudutaksid PS §-s 104 toodud Riigikogu koosseisu häälteenamuse nõuet.

2. Seaduse eesmärk

Eelnõu eesmärk on tõhustada finantspettuste avastamist, väljaselgitamist ja tõkestamist, andes makseteenuse pakkujatele selge õigusliku aluse maksejuhise täitmisest keeldumiseks ning krediidiasutustele õiguse jagada pettuse kahtluse korral vajalikku teavet teiste krediidiasutuste, PPA ning RIA-ga.

Kehtiv õigus ei võimalda finantspettuste kahtluse korral piisavalt kiiresti ja tõhusalt sekkuda, kuna maksejuhise täitmisest keeldumise õigus on kitsalt piiritletud. Samuti ei sisalda kehtiv õigus selgeid aluseid vajaliku ja õigeaegse info jagamiseks ning seeläbi ei toimi tõhusalt ka erinevate osapoolte omavaheline koostöö.

Üldjuhul töödeldakse makseid reaalajas, mis tähendab, et makse saaja kontole jõuavad need sekunditega. Eestis oli välkmaksete osakaal 2025. aasta juuli seisuga 87%[5]. Pettuse toimepanija jaoks tähendab see seda, et juhul kui saadakse isik pettuse teel makset tegema, laekub raha kohe petturi kontrolli all olevale maksekontole, tihtipeale nn rahamuula maksekontole, kust see järgmisesse riiki kantakse. Seetõttu on oluline, et makseteenuse pakkujatel oleks selge õiguslik alus maksejuhise täitmisest keeldumiseks ning väga oluline on andmete vahetamine erinevate osapoolte vahel.

[2] Directive - 2015/2366 - EN - Payment Services Directive - EUR-Lex
[3] https://eur-lex.europa.eu/eli/reg/2024/886/oj
[4] https://valitsus.ee/valitsuse-eesmargid-ja-tegevused/valitsemise-alused/koalitsioonilepe-2025-2027/riigirahandus
[5] maksete-ulevaade-2025_2-avalik.xlsx

Finantspettustega võitlemine on kesksel kohal ka Euroopa Liidu õigusloomes. Nimelt on Euroopa Liidu tasemel sisuliselt kokku lepitud uus makseteenuse määrus[6], mis hakkab asendama praegu kehtivat makseteenuste direktiivi 2015/2366[7]. Määrusega tugevdatakse muuhulgas makseteenuste turvalisust ning nähakse ette ulatuslikumad pettusevastased meetmed, mis aitavad makseteenuse pakkujatel kui ka vastavatel ametiasutustel tõhusamalt sekkuda pettuste avastamisse, väljaselgitamisse ja tõkestamisse. Määrus paneb muuhulgas makseteenuse pakkujatele kohustuse autoriseeritud maksete täitmisest keelduda juhul, kui on alus kahtlustada pettust. Samuti näeb määrus ette andmete vahetamise makseteenuse pakkujate vahel ning samuti muude asutustega. Makseteenuste määruse osas jõuti poliitilise kokkuleppeni 2025. aasta novembris[8]. Määrust hakatakse eeldatavalt kohaldama 2028. aasta lõpus.

Euroopa Liidu Nõukogu töögruppides oli üheks keskseks teemaks pettuste vastased meetmed uues makseteenuste määruses, sealhulgas ka pettuslike maksete blokeerimine ja andmete vahetamine makseteenuse pakkujate ning teiste asutuste vahel. Komisjoni esialgne ettepanek neid meetmeid ei sisaldanud, kuid arutelude käigus tõusetusid need kui väga olulised ja vajalikud meetmed pettustega võitlemisel. Erinevalt käesolevast eelnõust on uues makseteenuste määruses andmete vahetamine ja tehingute blokeerimine makseteenuse pakkujale kohustuslik.

Käesolev eelnõu lähtub samast eesmärgist ning loob riigisiseses õiguses vajalikud õiguslikud alused, mis aitavad pettusi tõhusamalt avastada, välja selgitada ja tõkestada. Eesmärk on võimaldada selliste meetmete rakendamist teatud ulatuses juba enne, kui hakkab kehtima uus makseteenuste määrus. Arvestades pettuste jätkuvat kasvu ning nende tekitatud suurt kahju nii isikutele kui ettevõtjatele, on põhjendatud rakendada sarnase sisuga meetmeid võimalikult varakult. Kui uus makseteenuse määrus hakkab kehtima, tuleb lähtuvalt sellest analüüsida ja tõenäoliselt kehtetuks tunnistada need siseriiklikud sätted, mis tulenevad otse eelnimetatud EL määrusest.

Seaduseelnõule ei ole koostatud väljatöötamiskavatsust ega ka õiguslikke valikuid kajastavat kontseptsiooni, kuna eelnõu käsitleb EL õiguse rakendamist ning EL õigusakti eelnõu menetlemisel on sisuliselt lähtutud HÕNTE § 1 lg 1 nõuetest. („Hea õigusloome ja normitehnika eeskirja“ § 1 lõike 2 punkt 2).

3. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb kolmest paragrahvist.

Eelnõu §-ga 1 muudetakse VÕS-i.

Eelnõu § 1 punktiga 1 täiendatakse VÕS § 711 lõiget 1 punktiga 15[1], mille kohaselt tuleb makseteenuse pakkujal esitada makseteenuse lepingu tingimustes igale kliendile maksejuhise

[6] EUR-Lex - 52023PC0367 - ET - EUR-Lex
[7] https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng
[8] https://www.europarl.europa.eu/news/en/press-room/20251121IPR31540/payment-services-deal-more-protection-from-online-fraud-and-hidden-fees

täitmise edasilükkamise tingimused tulenevalt käesoleva seaduse §-st 724^7. VÕS § 711 näeb ette teabe, mille peab makseteenuse pakkuja kliendile esitama makseteenuse lepingu tingimuste kohta. Kuivõrd makseteenuse pakkujal on õigus maksejuhise kättesaamist edasi lükata, siis sätestatakse seaduses, et sellest tuleb klienti teavitada. peab kliendil olema õigus sellest ja selle tingimustest ka ette teada. Seeläbi saab klient teada, et maksejuhise kättesaamise edasilükkamine ei ole makseteenuse pakkuja suvaotsus, vaid selline õigus tuleneb seadusest ning selle eesmärk on kaitsta klientide vara finantspettuste eest.

Eelnõu § 1 punktiga 2 täiendatakse VÕS-i §-ga 724^7, mis näeb ette lisaturvameetmete rakendamine pettusekahtluse korral.

Eelnõu § 1 punktiga 2 **VÕS-i lisatav § 724^7 lõige 1** näeb ette, millisel juhul on makseteenuse pakkujal õigus maksejuhise kättesaamine edasi lükata ja rakendada lisaturvameetmeid. Selline õigus on juhul, kui maksja makseteenuse pakkujal on objektiivselt põhjendatud kahtlus, et:
1) maksejuhist ei ole autoriseerinud maksja või
2) maksejuhis on autoriseeritud andmete väärkasutamise, pettuse või maksjaga manipuleerimise teel.

Järgnevalt on maksejuhise autoriseerimise ning maksejuhise kättesaaduks lugemise paremaks mõistmiseks välja toodud makseprotsessis autoriseerimise ja selle käigus toimuva pettuslike maksete tõkestamise tehnilisem kirjeldus.

Tegevused saab jagada kaheks – need, mis toimuvad enne PIN 2 sisestamist ning need mis pärast seda.

Esiteks on tegevused, mis toimuvad enne PIN 2 sisestamist. Esmalt isik kinnitab oma tavapäraste autentimisvahenditega logimise internetipanka (nt PIN 1, biomeetria). Juba internetipanka sisse logimisel on makseteenuse pakkuja kohustatud tegema tavapärast kontrolli ja riskihindamist. Kui isik soovib teha makset, on tinglikult võimalikud kolm erinevat lõpptulemust. Esiteks, makseteenuse pakkuja tuvastab juba internetipanka sisselogimise andmete põhjal pettuse kahtluse ning siis on võimalus kasutajatunnus või konto blokeerida. Teiseks, pettuse kahtlus tuvastatakse siis, kui isik täidab maksevormi. Sellisel juhul on võimalus keelduda makset kinnitamast juba enne PIN 2 sisestamist ning sellest teavitatakse klienti. Kolmandaks, pettusekahtlust ei ole ning isik kinnitab makse tavapäraselt PIN 2-ga. Eeltoodust tulenevalt asub sellisel juhul kontrolli kese monitooringus, mis tehakse enne PIN 2-ga maksejuhise kinnitamist ehk et tehingu autoriseerimine ei ole tehniliselt veel lõppenud.

Teiseks on tegevused, mis toimuvad pärast PIN 2 sisestamist. Sellisel juhul on maksejuhise autoriseerimine tehniliselt lõpuni viidud, kuid sellest hoolimata võib ka siis tekkida või kinnitust leida objektiivselt põhjendatud pettusekahtlus ning peab olema võimalus sellise maksejuhise täitmisest keelduda. Pärast PIN 2 sisestamist on makseteenuse pakkujal võimalus rakendada mitmeastmelist kontrolli. Kui tekib pettusekahtlus edastatakse näiteks isikule teavitus, et makse suunatakse täiendavasse tehnilisse kontrolli, nt biomeetria kontroll või mõni muu lisaverifitseerimise meetod. Pärast täiendavat maksejuhise kontrolli on võimalik kaks olukorda. Esiteks, kui pettusekahtlus saab maandatud ning autoriseerimine loetakse lõppenuks,

ja asutakse maksejuhist täitma. Teiseks, kui pettusekahtlust ei ole olnud võimalik kõrvaldada ja keeldutakse maksejuhise täitmisest.

Kehtiv õigusraamistik võimaldab makseteenuse pakkujatel pettuste tõkestamisse maksejuhise täitmisel kõige tõhusamalt sekkuda enne PIN 2 sisestamist, ehk et tehniliselt enne autoriseerimise lõppemist. Makseteenuse pakkujate kohustus avastada autoriseerimata või pettuse teel tehtud maksetehinguid ei lõpe aga ühes PIN 2 sisestamisega, vaid ka pärast seda. Eelnõu annab siinkohal makseteenuse pakkujatele selge õigusliku aluse ja kriteeriumid, et sekkuda pettuse kahtluse puhul maksetehingu täitmisesse pärast PIN 2 sisestamist.

VÕS-i lisatava § 724[7] lõike 1 kohaselt tekib makseteenuse pakkujal õigus maksejuhise kättesaamine edasi lükata ja lisaturvameetmeid rakendada juhul, kui tal esineb objektiivselt põhjendatud kahtlus, et maksejuhist ei ole autoriseerinud maksja või maksejuhis on autoriseeritud andmete väärkasutamise, pettuse või maksjaga manipuleerimise teel, mis tähendab, et kahtlus peab tuginema konkreetsetele asjaoludele ja riskinäitajatele. Objektiivselt põhjendatud kahtlus võib muu hulgas tugineda näiteks järgmistele asjaoludele:

- maksejuhis erineb oluliselt maksja tavapärasest maksekäitumisest (nt ebatavaliselt suur summa ning uus makse saaja, ebatavaline kellaaeg või geograafiline asukoht);
- makse tegemisel kasutatakse seadmeid, IP-aadresse või autentimisviise, mis erinevad maksja tavapärasest kasutusmustrist;
- makseteenuse pakkuja tehinguseiremehhanismid tuvastavad tehingus mustreid, mis on iseloomulikud pettustele või andmete väärkasutusele;
- makse on seotud teadaolevate või kõrgendatud riskiga maksekontode, isikute või tegevustega;
- maksja käitumine viitab pettusele, nt ebatavaline maksete tegemise kiirus, korduvad katsed, vastuolulised sisestused, korraga kõikide maksete limiitide tõstmine.

Seejuures tuleb hinnata kõiki asjaolusid kogumis ning üksik riskitegur ei pruugi alati olla piisav maksejuhise kättesaamise edasilükkamiseks, et rakendada lisaturvameetmeid. Oluline on, et makseteenuse pakkuja tegevus oleks proportsionaalne ja põhjendatud – objektiivse kahtluse olemasolu peab olema dokumenteeritav ning vajaduse korral hiljem kontrollitav. Kehtiv VÕS § 733[4] lõige 1 näeb ette, e kui on vaieldav, kas maksetehing on autoriseeritud või nõuetekohaselt täidetud, peab makseteenuse pakkuja või asjakohasel juhul makseteenuse pakkuja, kelle makse algatamise teenuse kaudu makse algatati, tõendama, et maksetehing on autenditud, muu hulgas rakendatud kliendi tugevat autentimist, korrektselt dokumenteeritud ja kontodel kajastatud ning tehingu tegemist ei ole mõjutanud ükski puudus. See tagab, et makseteenuse pakkuja ei kasuta talle antud õigust meelevaldselt, vaid üksnes juhtudel, kus see on maksete turvalisuse tagamiseks vältimatult vajalik. Võib eeldata, et makseteenuse pakkujate huvides ei ole ka nimetatud meetme kergekäeline rakendamine, sest see mõjutab negatiivselt kliendi kogemust teenuse kasutamisel ning võib viia kliendi teise makseteenuse pakkuja pakutavate teenuste juurde.

Eelnõuga lisatav säte toob eraldi välja **kaks peamist olukorda**, mille esinemisel võib makseteenuse pakkuja **maksejuhise kättesaamise edasilükkamise õigust kasutada.**

Esiteks, on õigus maksejuhise kättesaamine edasi lükata **VÕS-i lisatava 724[7] lõike 1 punkti 1** kohaselt juhul, kui on põhjendatud kahtlus, et maksejuhist ei ole autoriseerinud maksja. See hõlmab olukordi, kus makse võib olla tehtud ilma maksja teadmise või nõusolekuta, näiteks juhul, kui kolmas isik on saanud ligipääsu maksja autentimisvahenditele või maksekontole. Ehk et tegemist on kehtiva VÕS-i järgi autoriseerimata maksega. VÕS § 724[1] lõige 1 sätestab, et maksetehing on maksjale siduv, kui ta on selle täitmiseks andnud nõusoleku. Nõusoleku võib anda enne tehingu tegemist või poolte kokkuleppel ka tagantjärele heakskiiduna. See tähendab, et juhul, kui makse on tehtud, kasutades kadunud või varastatud makseinstrumenti, on tegemist autoriseerimata maksega, sest puudub isiku nõusolek sellise makse tegemiseks.

Makseteenuste direktiivi artikli 64 lõike 1 kohaselt peavad liikmesriigid tagama, et maksetehing loetakse autoriseerituks üksnes siis, kui maksja on andnud nõusoleku maksetehingu täitmiseks, maksja võib sealjuures autoriseerida makse enne maksetehingu täitmist või maksja ja tema makseteenuse pakkuja vahelise kokkuleppe korral pärast maksetehingu täitmist (heakskiit). Artikli 64 lõike 4 kohaselt määratakse nõusoleku andmise viis ja kord poolte kokkuleppega. Sama artikli lõike 2 teises lauses on peetud oluliseks rõhutada, et kui mainitud „nõusolek" puudub, loetakse maksetehing „autoriseerimata maksetehinguks". Põhimõtteliselt võtab see mõistemääratlus hilisemates makseteenuse kasutaja ja makseteenuse pakkuja vastutuse sätetes kokku juhtumid, kus puudub maksejuhis või selle jõustumise täiendava eeldusena maksja nõusolek (maksevahendi kasutamise kaudu) makse tegemiseks. Sellisel juhul rakendub maksetehingu tegemise korral makseteenuse kasutaja ja makseteenuse pakkuja vastutus (st toimus autoriseerimata maksetehing). Maksja „nõusolekut" reguleeriv säte on rakendatav juhul, kui maksejuhise andmiseks kasutatakse mõnda maksevahendit, ülekannete puhul loetakse maksejuhis jõustunuks, kui see on kätte saadud (vt VÕS § 724[2]), ehk et „nõusolek" langeb kokku maksejuhise kättesaamise hetkega. Küll aga vaadeldakse „autoriseerimata maksena" seega nii makset, mille tegemiseks puudus maksejuhis, kui ka makset, mille tegemiseks puudus maksja „nõusolek". Mõlemal juhul rakendub vastutus makseteenuse eest „autoriseerimata" maksete korral. Kokkuvõtteks on makse autoriseerimise kontseptsioon „maksele nõusoleku andmine".

Kui tegemist on maksja enda antud maksejuhisega (nt isik teeb ise elektroonilise makse), siis sisaldub nõusolek maksetehingu tegemiseks juba iseenesest maksejuhises. Kui tegemist on saaja kaudu algatatud maksega (nt algatab kaupmees makse korduvate tellimuste puhul, kui maksja on andnud eelnevalt selleks nõusoleku), väljendub nõusolek maksevahendi kasutamises (VÕS § 724[1] lg 3). Nendel juhtudel annab maksja selgelt ja üheselt mõistetavalt oma nõusoleku enne maksetehingu täitmist, hilisema heakskiidu järele puudub vajadus, puudub ka võimalus jätta nõusolek andmata ning autoriseerida makse heakskiiduga. Seega on autoriseerimine hilisema heakskiidu andmise näol mõeldav üldiselt vaid saaja poolt algatatud maksetehingute puhul.

Teiseks, on õigus maksejuhise kättesaamine edasi lükata **VÕS-i lisatava 724[7] lõike 1 punkti 2** kohaselt juhul, kui maksejuhis on küll formaalselt autoriseeritud, kuid see on toimunud andmete väärkasutamise, pettuse või maksjaga manipuleerimise tulemusena. Siia alla kuuluvad näiteks juhtumid, kus maksjat on eksitatud (nt sotsiaalse manipulatsiooni teel) tegema makset, mida ta ei oleks teinud, kui tal oleks olnud asjaolude kohta õige teave. Tsiviilseadustiku üldosa seaduse (edaspidi *TsÜS*) § 94 lõike 1 kohaselt on pettus isiku tahtlik eksimusse viimine või

eksimuses hoidmine temale ebaõigete asjaolude avaldamise teel, eesmärgiga kallutada isik tehingut tegema. Sama paragrahvi lõike 2 kohasel on ebaõigete asjaolude avaldamisega võrdsustatud nendest asjaoludest teatamata jätmine, millest vastavalt hea usu põhimõttele oleks tulnud teatada, samuti selliste asjaolude tõesena avaldamine, mille tõele vastavust avaldaja ei ole kontrollinud ja mis hiljem osutuvad ebaõigeks.

Sellised olukorrad on pettuste toimepanemisel praktikas sagenenud ning nende puhul ei pruugi pelgalt autoriseerimise fakt tähendada seda, et isik ka tegelikult soovis sellist makset teha olukorras, kus talle esitati ebaõigeid asjaolusid ja viidi seeläbi isik eksimusse ning selle tulemusel andis isik nõusoleku maksetehingu tegemiseks, kui õigete asjaolude teadmisel ei oleks ta sellist kinnitust andnud.

Maksejuhise kättesaamise ajutiselt edasi lükkamise vaatest on oluline see, et mida pidada täpsemalt silmas maksejuhise kättesaamise all. Makseteenuste direktiivi artikkel 78 lõige 1 sätestab, et liikmesriigid tagavad, et laekumise ajaks on aeg, mil maksekäsund laekub maksja makseteenuse pakkujale. Kättesaamise konkreetse ajahetke määratlemine on oluline seepärast, et sellest alates hakkavad kulgema erinevad tähtajad (maksejuhise täitmine ja täitmisest keeldumise teate esitamine vt VÕS § 724[3], § 728). Oluline on see, et konkreetse ajahetke kaudu määratletakse arvelduspäev, millest järgneval saaja arvelduspäeval tuleb VÕS § 728 lõike 1 järgi maksejuhis täita (T+1 põhimõte).

Tegemist on kõrvalekaldega TsÜS §-ist 135 tähtaja kulgemise alguse regulatsioonist, sest T+1 eeldab, et kättesaamisele järgneval päeval oleks maksejuhis täidetud. Maksejuhise kättesaamine on samastatav põhimõtteliselt TsÜS § 69 regulatsiooniga ja tahteavalduse jõustumise kontseptsiooniga. TsÜS § 69 lõike 1 kohaselt tuleb kindlale isikule suunatud tahteavaldus väljendada ja see muutub kehtivaks kättesaamisega.

Maksejuhise kui tahteavalduse jõustumisel ehk maksejuhise kättesaamisel võib tegemist olla nii eemalviibijale kui kohalviibijale tehtud tahteavalduse jõustumisega. Eemalviibijale tehtava tahteavaldusega on tegemist juhul, kui maksejuhise andmine toimub kasutades mõnd elektroonilist vahendit (nt ülekanne internetipangas, kaardimakse jms), mis ei võimalda reeglina vahetut dialoogi tahteavalduse tegija (maksja) ja saaja (makseteenuse pakkuja) vahel. Kohalviibijale tehtud tahteavaldusega on tegemist siis, kui maksejuhis antakse pangakontoris pangatellerile. Kohalviibijale tehtud tahteavaldus jõustub isiklikult teatavaks tegemisega ehk siis hetkel, mil maksja teeb maksejuhise pangatellerile teatavaks, loetakse maksejuhis kättesaaduks. Kohalviibijale antava maksejuhise ajahetk on seega kindlalt ja üheselt määratletav.

Eemalviibijale antava maksejuhise puhul on olukord keerulisem. TsÜS § 69 lõike 2 kohaselt loetakse eemalviibijale tehtud tahteavaldus kättesaaduks, kui see jõuab eemalviibija asukohta ja tahteavalduse saajal on mõistlik võimalus sellega tutvuda. Kättesaamine toimub siis, kui tahteavaldus on jõudnud avalduse saaja mõjusfääri, nii et tal on objektiivselt võimalik tahteavalduse sisust teada saada ning tavapärastel oludel võib tahteavaldusest teadasaamisega arvestada.[9]

[9] Liis Hallik, Tahteavaldus tsiviilõiguses, Magistritöö, 2005, lk 88, viide 248 Brox'ile

Valitseva arvamuse kohaselt on tahtevalduse kättesaamise hetkeks see hetk, mil tahteavalduse adressaadil oleks normaalsetes oludes võimalus tahteavalduses toodud teave omaks võtta. Kui adressaat tutvub teabega varem, kui seda võiks temalt mõistlikult oodata, siis loetakse, et tahteavaldus on teabega tutvumise ajal kätte saadud.[10]

Maksejuhise laekumise aja kindlaksmääramisel ei lähe arvesse võimalik eelnev maksejuhise kättesaamiseks ja töötlemiseks ettevalmistav protsess (näiteks erinevate turva- ja kaitsenõuete täitmine).[11] Olenevalt maksejuhise esitamise kanalist (internetipank, pangakontor) viiakse osa kontrollidest läbi juba enne maksejuhise vastuvõtmist ning puudustest teavitatakse maksejuhise saatjat kohe.

Maksejuhise töötlemiseks ja kättesaamiseks vajaliku ettevalmistava protsessi lugemine kättesaamisele eelnevale ajale langevaks tegevuseks, on sisuliselt TsÜS-i § 69 lõike 2 lause 2 tahteavaldusega tutvumiseks mõistliku võimaluse jätmise ja erinevate kättesaamisteooriate väljendus maksejuhise kättesaamise kontekstis.

Maksejuhise kui tahteavalduse sisust teadasaamiseks ei saa lugeda aega, mil toimub erinevate formaalsete ja tehniliste nõuete täitmine. Sellisel ajahetkel ei tegeleta veel maksejuhise kui tahteavalduse sisuga, vaid maksejuhise tehnilise, formaalse ning välise poolega. Seega tuleb maksejuhise kättesaamise hetke kindlaksmääramisel arvestada võimalust maksejuhise sisuga tutvuda.

Maksejuhise kättesaamise hetkeks tuleks lugeda hetke, mil on juba eelnevalt tuvastatud, et maksejuhis vastab tehnilistele nõuetele ja täidetud on vajalikud kriteeriumid turvanõuete järgimiseks ning seda on võimalik täitma hakata. Maksejuhise võib kättesaaduks lugeda siis, kui on võimalik tutvuda maksejuhise sisuga ja kui seda on võimalik sisuliselt täita.

Makseteenuse pakkujad peavad kasutama autentimisel ning rahaliste vahendite kinnitamise ja piiramise ning samuti makse algatamise teenuse ja kontoteabe teenuse osutamise korral turvalist teabevahetamise viisi ning rakendama turvameetmeid, mis tagavad isikustatud turvaelementide konfidentsiaalsuse ja andmete tervikluse (VÕS § 724^6 lõige 1). Sama paragrahvi lõige 2 näeb ette, et täpsemad nõuded käesoleva paragrahvi lõikes 1 nimetatud turvalise teabevahetuse ja turvameetmete kohta kehtestatakse Euroopa Parlamendi ja nõukogu direktiivi 2015/2366/EL (edaspidi *komisjoni rakendusmäärus*) artiklis 98 nimetatud Euroopa Komisjoni rakendusmäärusega.

Komisjoni rakendusmääruse artikli 2 lõike 1 kohaselt peavad makseteenuse pakkujatel turvameetmete rakendamise eesmärgil olema tehinguseiremehhanismid, mis võimaldavad neil avastada autoriseerimata või pettuse teel tehtud maksetehinguid. Need mehhanismid peavad tuginema maksetehingute analüüsile, mille juures võetakse arvesse elemente, mis on makseteenuse kasutajale iseloomulikud isikustatud turvavolituste tavapärase kasutamise puhul.

[10] D. Einsele, Münchener Kommentar, BGB, Band I Allgemeiner Teil, § 130, Verlag C. H. Beck, München 2001, S. 1254
[11] Saksamaa BGB muutmise seaduse eelnõu seletuskiri, S 174

Komisjoni rakendusmääruse artikli 2 lõike 2 kohaselt tagavad makseteenuse pakkujad, et tehinguseiremehhanismid võtavad arvesse vähemalt kõiki järgmisi riskipõhiseid tegureid:

a) murtud või varastatud autentimisvahendite loetelu;
b) iga maksetehingu summa;
c) makseteenuste osutamisega seoses teada olevad petuskeemid;
d) märgid pahavaraga nakatumise kohta autentimismenetluse mis tahes seansi kestel;
e) juhul kui juurdepääsuseadme või -tarkvara annab kasutaja käsutusse makseteenuse pakkuja, logid sellise juurdepääsuseadme või -tarkvara kasutamise ning juurdepääsuseadme või -tarkvara tavapäratu kasutamise kohta.

Lisaturvameetmete rakendamine ei ole nii-öelda eraldi süsteem, vaid juba olemasolevate turvameetmete sihipärane täiendav kasutamine olukorras, kus tekib kahtlus, et maksejuhis ei ole maksja poolt autoriseeritud või maksejuhis on autoriseeritud andmete väärkasutamise, pettuse või maksjaga manipuleerimise teel. Lisaturvameetmete rakendamise sisu on konkreetse maksejuhise täiendav kontroll pettuse tõkestamise eesmärgil, kui tehingu riskianalüüsi põhjal tekib eelnevalt nimetatud kahtlus, ehk et risk on tavapärasest suurem.

Makseteenuste direktiiv on artikli 107 kohaselt üldjuhul maksimumharmoniseeriv, mistõttu ei saa liikmesriik kehtestada direktiivis sätestatust teistsugust regulatsiooni. Käesolev eelnõu ei lähtu sellest, et makseteenuse pakkujal oleks õigus juba kättesaadud ja autoriseeritud maksejuhise täitmine ühepoolselt peatada. Eelnõu täpsustab olukorda, kus makseteenuse pakkuja peab enne maksejuhise kättesaamist teostama kontrolli, kas maksejuhis vastab kõikidele vastuvõtmise tingimustele, sealhulgas kas tegemist on maksja poolt autoriseeritud maksejuhisega ning kas tegemist ei ole olukorraga, kus makse on autoriseeritud andmete väärkasutamise, pettuse või maksjaga manipuleerimise teel. Ehk tegemist on maksejuhise täiendava kontrolliga selle vastuvõtmise eelses faasis.

Makseteenuse pakkuja poolt rakendatavad lisaturvameetmed võivad hõlmata näiteks maksjaga ühenduse võtmist, et välja selgitada, kas maksejuhise on esitanud ikka isik ise või kas teda on manipuleeritud sellist makset tegema. Samuti muud kontrollid, näiteks makse saaja makseteenuse pakkujaga info vahetamine, et välja selgitada, kas konkreetne maksekonto võib olla seotud pettuste toimepanemisega. Meetmete täpne sisu ja ulatus sõltub konkreetsest olukorrast ning maksega seotud riskist. Oluline on hinnata kõiki asjaolusid ja koguda vajadusel täiendavat teavet. Üksik riskitegur ei pruugi olla piisav asjaolude väljaselgitamiseks. Eeltoodust tulenevalt saab lisaturvameetmeid käsitada laia mõistena, mis hõlmab nii tehnilisi, organisatsioonilisi kui ka menetluslikke meetmeid, mille eesmärk on maksete turvalisuse tagamine ja pettuste ennetamine.

Makseteenuste direktiivi artikli 64 kohaselt loetakse maksetehing autoriseerituks üksnes siis, kui maksja on andnud nõusoleku maksetehingu tegemiseks. Sellest tulenevalt ei pea makseteenuse pakkuja pettusekahtluse korral piirduma üksnes formaalse autentimise fakti tuvastamisega, vaid tal peab olema võimalik hinnata, kas tehniline autoriseerimise fakt väljendab tegelikku nõusolekut. Seda kinnitab ka kehtiv VÕS § 733^4 lõige 2, mis sätestab, et kui on vaieldav, kas makseinstrumendi abil tehtud maksetehing on autoriseeritud, ei ole

ainuüksi makseinstrumendi kasutamise dokumenteerimine makseteenuse pakkuja ja asjakohasel juhul makse algatamise teenust osutanud makseteenuse pakkuja poolt küllaldane selle tõendamiseks, et: 1) maksetehing on autoriseeritud; 2) makseinstrumenti on kasutatud pettuse teel; 3) rikutud on ühte või mitut käesoleva seaduse §-s 733[10]sätestatud nõuet või 4) rikutud on tahtlikult või raske hooletuse tõttu ühte või mitut makseinstrumendi väljastamise ja kasutamise tingimust.

Euroopa Pangandusjärelevalve on 2025. aasta vastuses küsimusele „2023_6873 PISP payment order cancellation due to fraud prevention reasons“[12] selgitatud, et juhul, kui enne maksejuhise täitmist tekib küsimus, kas see oli üldse autoriseeritud, peab kontot haldav makseteenuse pakkuja olemasolevate elementide põhjal hindama, kas tehing oli autoriseeritud või mitte. Seda toetavad koosmõjus makseteenuste direktiivi artiklid 78 ja 83. Artikkel 78 seob maksejuhise kättesaamise aja hetkega, mil maksejuhis jõuab maksja makseteenuse pakkujani, ning artikkel 83 seob makse täitmise tähtaja selle kättesaamise hetkega. Komisjoni rakendusmäärus lähtub riskipõhisest kontrollist ja näeb ette, et makseteenuse pakkujad rakendavad tehingute riskianalüüsi, et tuvastada volitamata või pettuslikke tehinguid. Seetõttu on põhjendatud lisaturvameetmete rakendamine olukorras, kus makseteenuse pakkujal on objektiivselt põhjendatud kahtlus, et maksejuhis ei ole maksja poolt autoriseeritud või on autoriseeritud andmete väärkasutamise, pettuse või maksjaga manipuleerimise teel. Kui makseteenuse pakkuja on selle kontrolli tulemusel veendunud, et maksejuhis ei ole autoriseeritud andmete väärkasutamise, pettuse või maksjaga manipuleerimise teel, tuleb maksejuhis viivitamata saata edasi makse saaja makseteenuse pakkujale.

Makseteenuste direktiivi maksete autoriseerimise regulatsioon ning komisjoni rakendusmääruse nõuded kehtivad ka välkmaksetele. Välkmaksete määruse kohaselt peab maksja makseteenuse pakkuja kohe pärast välkmaksejuhise kättesaamist kontrollima, kas makse töötlemise tingimused on täidetud ja kas vajalikud vahendid on olemas, ning saatma maksetehingu viivitamata saaja makseteenuse pakkujale. Välkmaksete määruse kohaselt olenemata direktiivi (EL) 2015/2366 artiklist 83 (eelnevalt välja toodud selgitus maksejuhise täitmise T+1 põhimõte), kontrollib maksja makseteenuse pakkuja viivitamata pärast välkkreeditkorralduse maksekäsundi vastuvõtmise aega, kas kõik maksetehingu töötlemiseks vajalikud tingimused on täidetud ja kas vajalik raha on kättesaadav, reserveerib maksetehingu summa maksja kontol või debiteerib selle maksja kontolt ja saadab maksetehingu viivitamata makse saaja makseteenuse pakkujale.

Välkmaksete määruse kohaselt (artikkel 5c lõige 1) pakub maksja makseteenuse pakkuja maksjale teenust, millega tagatakse selle makse saaja kontrollimine, kellele maksja kavatseb kreeditkorralduse saata (edaspidi „makse saaja kontrollimise teenus“). Maksja makseteenuse pakkuja osutab makse saaja kontrollimise teenust viivitamata pärast seda, kui maksja esitab asjakohase teabe makse saaja kohta, ja enne seda, kui maksjale pakutakse võimalust kõnealune kreeditkorraldus autoriseerida. Selle kohaselt peab maksja makseteenuse pakkuja kontrollima, kas makse töötlemise tingimused on täidetud enne maksejuhise autoriseerimist. Juhul, kui maksja makseteenuse pakkujal tekib autoriseerimise protsessi käigus objektiivselt põhjendatud kahtlus, et maksejuhis ei ole maksja poolt autoriseeritud või on autoriseeritud andmete

[12] 2023_6873 PISP payment order cancellation due to fraud prevention reasons | European Banking Authority

väärkasutamise, pettuse või maksjaga manipuleerimise teel, on võimalik enne maksejuhise kättesaamist rakendada täiendavat kontrolli.

Juhul, kui makseteenuse pakkujal ei oleks õigust välkmakse maksejuhise vastuvõtmist edasi lükata ning vajadusel selle täitmisest keelduda, siis olukorras, kus makseteenuse pakkujal on objektiivselt põhjendatud kahtlus, et maksejuhist ei ole autoriseerinud isik ise ja seda tehti näiteks andmete väärkasutamise teel, ning selline maksejuhis täidetakse, siis vastutab makseteenuse pakkuja autoriseerimata maksega tekitatud kahju eest.

Kehtivas õiguses on makseteenuse pakkujatele pandud kohustus (komisjoni rakendusmäärus artikkel 2) omada tehinguseiremehhanisme, mis võimaldavad neil avastada autoriseerimata või pettuse teel tehtud maksetehinguid. Pettuste vastu võetavad meetmed võib tinglikult jagada kolmeks. **Esiteks** on ennetavad tehnilised meetmed, nagu näiteks kliendi tugev autentimine ning turvalised autentimisvahendid. **Teiseks** on erinevad kontrollimeetmed, nagu tehingute reaalaajas riskianalüüs, mis peab arvestama näiteks erinevaid maksemustreid, isiku ebatavalist käitumist jne. **Kolmandaks** saab pidada sekkuvaid meetmeid, ehk meetmed mida saab võtta siis, kui on tuvastatud pettusekahtlus, ning vajalikud on riske maandavad meetmed nagu näiteks maksetehingu täitmisest keeldumine. Praegu on olukord, kus seaduses sätestatud sekkumist lubavad meetmed ei ole pettuste tõkestamiseks piisavad. Ilmselgelt ei ole võimalik läbi ennetavate ja kontrollmeetmete rakendamise ära hoida kõiki pettusi. Samuti ei ole võimalik kõiki pettusi ära hoida lisaks eelnevatele ka erinevate sekkumismeetmega, kuid nende olemasolu on siiski selle eesmärgi saavutamisel oluline. Seepärast on vajalik seaduses sätestada makseteenuse pakkujatele selge alus pettusekahtluse korral rakendada maksejuhise osas lisaturvameetmeid. Kui komisjoni rakendusmääruses on makseteenuse pakkujatele peale pandud kohustus avastada autoriseerimata või pettuse teel tehtud tehinguid, siis peavad selle eesmärgi täitmiseks olema ka asjakohased meetmed, mis takistavad selliste maksetehingute tegemist.

Komisjoni rakendusmääruse põhjenduspunkt 1 näeb ette, et „Elektrooniliselt pakutavad makseteenused tuleks teostada turvaliselt, võttes kasutusele tehnoloogia, mis suudab tagada kasutaja turvalise autentimise ja vähendada maksimaalselt pettuse ohtu. Autentimismenetlus peaks üldiselt hõlmama mehhanisme tehingute seireks, et tuvastada katseid kasutada makseteenuse kasutaja isikustatud turvavolitusi, mis on kaotatud või varastatud või mida on väärkasutatud; samuti tuleks sellega tagada, et makseteenuse kasutaja on seaduslik kasutaja ja annab seega isikustatud turvavolitusi tavapärasel viisil kasutades oma nõusoleku rahaliste vahendite ülekandmiseks ja oma kontoandmetele juurdepääsuks. Lisaks tuleb kindlaks määrata nõuded seoses kliendi tugeva autentimisega, mida tuleks kasutada iga kord, kui maksja siseneb interneti kaudu oma maksekontole, algatab elektroonilise maksetehingu või teeb kaugejuurdepääsu teel mis tahes muu toimingu, mille puhul võib esineda maksepettuse või muu kuritarvitamise oht, nõudes selliste autentimiskoodide genereerimist, mille puhul ei ole ohtu, et neid saaks kas tervikuna või mõne nende genereerimiseks kasutatud elemendi avalikustamise läbi võltsida.“. Makseteenuste direktiivi ja komisjoni rakendusmäärusega makseteenuse pakkujatele pandud üldine kohustus on ennetada pettusi ja hinnata maksetega seotud riske ning makseteenuse pakkuja peab rakendama asjakohaseid turvameetmeid eelkõige olukordades, kus maksetehing võib kaasa tuua pettuse või muu väärkasutuse riski. Üheks selle eesmärgi

saavutamise vajalikuks osaks on ka maksejuhise vastuvõtmise edasilükkamine, mis võimaldab nimetatud eesmärki saavutada. Komisjoni rakendusmäärus kehtib ka välkmaksete puhul.

Eelnõu § 1 punktiga 2 VÕS-i lisatav 724[7] lõige 2 näeb ette, millel peab objektiivselt põhjendatud kahtlus põhinema ning millised asjaolud iseseisvalt ei ole piisavad maksejuhise kättesaamise edasilükkamiseks.

Sätte kohaselt peab objektiivselt põhjendatud kahtlus põhinema makseteenuse pakkuja riskihindamisel, sealhulgas Euroopa Parlamendi ja nõukogu direktiivi 2015/2366/EL 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 (ELT L 337, 23.12.2015, lk 35–127) artiklis 98 nimetatud Euroopa Komisjoni rakendusmääruses (edaspidi *komisjoni rakendusmäärus*) sätestatud riskipõhisel lähenemisel ning muudel objektiivsetel asjaoludel. Makseteenuse pakkujad peavad hindama maksetega seotud riske, võttes arvesse muu hulgas näiteks maksja käitumismustreid, tehingu iseloomu ning võimalikke pettusenäitajaid. Seega lähtub kavandatav regulatsioon samast põhimõttest, mille kohaselt ei ole kõik maksed nii öelda selle poolest „võrdsed“, vaid neid hinnatakse lähtuvalt konkreetsest riskitasemest.

Komisjoni rakendusmääruse artikkel 18 käsitleb olukorda, kus makseteenuse pakkujatele antakse luba mitte kasutada kliendi tugevat autentimist juhul, kui maksja algatab elektroonilise kaugmaksetehingu, mille makseteenuse pakkuja tehinguseiremehhanismide alusel lugenud väikese riskiga tehinguks. See artikkel küsitleb küll tehingu riskianalüüsi olukorras, kus on ette nähtud erand kliendi tugeva autentimise kohustusest, kuid see artikkel piltlikustab, milliseid asjaolusid tuleb muuhulgas näiteks reaalajas toimuva riskianalüüsi käigus hinnata.

Hinnata tuleb näiteks seda, kas makseteenuse pakkujad ei ole reaalajas toimuva riskianalüüsi tulemusena avastanud ühtegi järgmistest asjaoludest: a) maksja tavapäratud kulutused või käitumismuster; b) ebatavaline teave maksja seadme/tarkvara kasutamise kohta; c) pahavaraga nakatumine autentimismenetluse mis tahes seansi kestel; d) makseteenuste osutamisega seoses teadaolev petuskeem; e) maksja tavapäratu asukoht; f) makse saaja kõrge riskitasemega asukoht.

Kehtiv VÕS ei näe otseselt ette, et juhul, kui makseteenuse pakkujal tekib objektiivselt põhjendatud kahtlus, et maksetehingu täitmiseks antud nõusolek on saadud andmete väärkasutamise, pettuse või maksja manipuleerimise teel, on tal õigus autoriseeritud maksejuhise kättesaamine täiendavaks kontrolliks edasi lükata. Kehtiv VÕS § 724[3] lõige 4 sätestab, et makseteenuse pakkujal ei ole õigust keelduda autoriseeritud maksejuhise täitmisest, kui maksejuhis vastab makseteenuse lepingus määratud tingimustele ning maksejuhise täitmisega ei rikuta mõnes muus õigusaktis sätestatud kohustust. Kuid lisaks sellele, et maksejuhis peab vastama lepingus määratud tingimustele, peab maksejuhis vastama ka komisjoni rakendusmääruses kehtestatud nõuetele. Selles osas, et maksejuhise täitmisega ei rikuta mõnes muus õigusaktis sätestatud kohustusi, on eelkõige silmas peetud rahapesu ja terrorismi rahastamise tõkestamise regulatsioonist tulenevaid nõudeid. VÕS § 724[6] lõige 1 küll viitab autentimise nõuetele komisjoni rakendusmääruses, kuid ei anna selget õigust

maksejuhise täitmisest keelduda. Ehk et juhul, kui isik on makse autoriseerinud ka pettuse teel, ei ole VÕS § 724^3 lõike 4 kohaselt makseteenuse pakkujal õigust keelduda sellise maksejuhise täitmisest.

VÕS § 724^6 lõige 5 sätestab, et maksejuhist, mille täitmisest on õigustatult keeldutud, käsitatakse kättesaamata maksejuhisena tulenevalt käesoleva seaduse §-des 728 ja 733^3 sätestatust. See omab tähtsust nii maksejuhise täitmise tähtaja kui ka makseteenuse pakkuja vastutuse kontekstis. Kui maksejuhise täitmisest on õigustatult keeldutud, käsitatakse maksejuhist kättesaamata maksejuhisena, see tähendab, et maksejuhisest ei tulene makseteenuse pakkujale ega ka makseteenuse kasutajale mingeid õigusi ega kohustusi.

Lisatava lõike eesmärk on tagada, et makseteenuse pakkuja õigus maksejuhise kättesaamine edasi lükata oleks selgelt piiritletud ning ei võimaldaks maksejuhise põhjendamatut kättesaamisega viivitamist. Selleks sätestatakse, et kahtlus peab olema objektiivselt põhjendatud ning tulenema riskihindamisest või muudest objektiivsetest asjaoludest.

Eraldi on välja toodud, et makseteenuse pakkuja ei või maksejuhise kättesaamise edasi lükkamisel tugineda üksnes Euroopa Parlamendi ja nõukogu määruse (EL) nr 260/2012 alusel pakutavale makse saaja kontrollimise teenusele (nn IBAN-nime kontroll). Nimetatud teenuse eesmärk on anda maksjale lisateavet makse saaja kohta, kuid selle tulem ei pruugi olla lõplik ega ammendav ning võib sõltuda andmete kättesaadavusest või tehnilistest piirangutest. Seetõttu ei saa üksnes selle teenuse tulemusest järeldada, et maksejuhis ei ole maksja poolt autoriseeritud või maksejuhis on autoriseeritud andmete väärkasutamise, pettuse või maksjaga manipuleerimise teel.

Samuti ei ole piisav alus maksejuhise kättesaamise edasilükkamiseks asjaolu, et makse on makseteenuse pakkujale ebatavaline või arusaamatu. Kuigi maksejuhise ebatavalisus võib olla üks riskihindamise element, ei anna see iseseisvalt alust järeldada, et tegemist on nt pettuse või andmete väärkasutusega. Vastupidine käsitlus tooks kaasa olukorra, kus makseteenuse pakkujad võiksid laialdaselt ja ebamääraste kriteeriumide alusel maksete täitmisega viivitada. Oluline on, et makseteenuse pakkuja poolt maksejuhise kättesaamise edasilükkamine oleks erandlik ning selgelt põhjendatud. Kavandatava regulatsiooni eesmärk on tasakaalustada maksete turvalisuse ja kiiruse eesmärke ning samas mitte kahjustada maksete usaldusväärsust, võimaldades makseteenuse pakkujal maksejuhise kättesaamine edasi lükata üksnes siis, kui see on riskihindamise alusel põhjendatud, vältides samas põhjendamatuid viivitusi.

Eelnõu § 1 punktiga 2 VÕS-i lisatav 724^7 lõige 3 näeb ette, et makseteenuse leping peab sisaldama muu hulgas tingimusi maksja teavitamiseks lisaturvameetmete rakendamisest ja põhjustest enne nende rakendamist või viivitamata pärast seda. Makseteenuse pakkuja ei pea lisaturvameetmete rakendamise põhjusi maksjale teatama, kui teabe edastamine on vastuolus objektiivselt põhjendatud turvalisuse kaalutlusega või ei ole muul seaduses sätestatud põhjusel lubatud. Selline lähenemine on kooskõlas makseteenuste direktiivi põhimõtetega, et makseteenuse pakkuja peab ühelt poolt tagama makseteenuste läbipaistvuse ja kasutajate teavitamise, kuid teiselt poolt ka maksete turvalisuse ja pettuste ennetamise. Sarnane tasakaalu

leidmine on omane ka muudele menetlustele, kus isiku teavitamine võib olla piiratud, kui see ohustab turvalisust.

Lõike 3 eesmärk on tagada maksja teavitamine olukorras, kus makseteenuse pakkuja rakendab lisaturvameetmeid ja lükkab maksejuhise kättesaamise edasi. Kuna see võib mõjutada makse täitmise kiirust ja maksja ootusi selle täitmise osas, on oluline, et maksja oleks teadlik nii võimalikest meetmetest kui ka nende rakendamise tingimustest. Seeläbi saab isik teada, miks tema maksejuhise täitmine võib viibida või miks temalt nõutakse näiteks täiendavat informatsiooni. Teisalt kaitseb see ka makseteenuse pakkujat, kes saab tugineda seaduses sätestatule ning aitab vältida isikute arusaamist, et tegemist on makseteenuse pakkuja nn omavoliga.

Teavitamise kohustus hõlmab nii eelnevat kui ka vahetut teavitamist. Üldreeglina tuleks maksjat teavitada enne lisaturvameetmete rakendamist, võimaldades vajaduse korral maksjal täiendavaid selgitusi anda. Kui eelnev teavitamine ei ole võimalik, näiteks seetõttu, et turvameetme tõhusus eeldab viivitamatut sekkumist, tuleb maksjat teavitada viivitamata pärast nende meetmete rakendamist. Selline paindlikus võimaldab makseteenuse pakkujal reageerida pettustele kiiresti, kuid säilib maksja teadlikus olukorra põhjustest.

Säte tagab, et maksja ei jää teadmatusse maksejuhiste täitmist mõjutavate tegurite osas, säilitades samas võimaluse piirata teabe avaldamist juhtudel, kus see on vajalik maksete turvalisuse ja pettuste ennetamise seisukohalt.

Eelnõu § 1 punktiga 2 VÕS-i lisatav 724[7] lõige 4 näeb ette, et kui maksja makseteenuse pakkuja lükkab maksejuhise kättesaamise lisaturvameetmete rakendamiseks edasi, siis loetakse, et makseteenuse pakkuja on maksejuhise kätte saanud hetkest, kui makseteenuse pakkuja on lõpetanud lisaturvameetmete rakendamise ja on veendunud, et maksejuhis ei ole autoriseeritud andmete väärkasutamise, pettuse või maksjaga manipuleerimise teel. Nimetatud tingimuste täitmise korral on maksja makseteenuse pakkujal kohustus saata maksetehing viivitamata makse saaja makseteenuse pakkujale.

Nimetatud lõige näeb ette, millisest hetkest alates loetakse maksejuhis makseteenuse pakkuja poolt kättesaaduks olukorras, kus makse täitmine ei alga kohe selle kättesaamisel, vaid sellele eelneb täiendav riskipõhine kontroll. Kehtivas makseteenuste regulatsioonis on maksejuhise kättesaamise hetk keskse tähtsusega, kuna sellest sõltuvad nii makse täitmise tähtajad kui ka makseteenuse pakkuja vastutus. Seetõttu on oluline vältida olukorda, kus makseteenuse pakkuja oleks kohustatud järgima täitmise tähtaegu ajal, mil ta ei ole veel saanud veenduda, kas maksejuhis on maksja poolt autoriseeritud või on see autoriseeritud andmete väärkasutamise, pettuse või maksjaga manipuleerimise teel. Kuigi makseteenuste direktiiv ja välkmaksete määrus eeldab maksete kiiret täitmist, ei saa seda igas olukorras tõlgendada viisil, mis kohustaks makseteenuse pakkujat täitma maksejuhiseid olukorras, kus esineb põhjendatud kahtlus, et need on toime pandud pettuse teel.

Lõike 4 kohaselt loetakse maksejuhis kättesaaduks alles pärast seda, kui makseteenuse pakkuja on lõpetanud lisaturvameetmete rakendamise ning on veendunud, et maksejuhis ei ole seotud

andmete väärkasutamise, pettuse või maksjaga manipuleerimisega. See tagab, et makse täitmise tähtaegade arvestus algab alles hetkest, mil makseteenuse pakkuja on pärast vajalike kontrollide tegemist saanud asuda sisuliselt maksejuhist täitma.

Lõikes 4 on selgelt välja toodud, et pärast lisaturvameetmete rakendamise lõppu ning kahtluste kõrvaldamist on makseteenuse pakkujal kohustus edastada maksetehing viivitamata makse saaja makseteenuse pakkujale. Välkmaksete kontekstis on oluline, et makseteenuse pakkuja sekkumine maksejuhise täitmisesse selle kättesaamisega edasilükkamisega toimuks üksnes enne makse lõplikku töötlemist ning oleks ajaliselt selgelt piiritletud.

Eelnõu § 1 punktiga 2 VÕS-i lisatav 724[7] lõige 5 näeb ette, et maksja makseteenuse pakkuja ei või maksejuhist lisaturvameetmete rakendamiseks edasi lükata kauemaks, kui käesoleva paragrahvi lõikes 4 nimetatud asjaolu väljaselgitamiseks mõistlikult vajalik. Võimalusel peab maksja makseteenuse pakkuja lähtuma eelkõige käesoleva seaduse §-s 728 sätestatud tähtaegadest. Nimetatud lõige sätestab lisaturvameetmete rakendamise ajapiiri kontrollimaks, kas maksejuhis vastab kõikidele selle töötlemiseks vajalikele nõuetele ega ole seotud andmete väärkasutamise, pettuse või maksjaga manipuleerimisega. See tähendab, et lähtepunktiks jäävad üldised täitmise tähtajad ning nendest võib eemalduda ainult nii palju, kui konkreetne kontrolli vajadus seda tingib. Eesmärk on tagada, et lisaturvameetmete rakendamise õigus ei oleks ajaliselt piiritlemata, vaid oleks seotud konkreetse kontrollivajaduse ja selle kestusega.

Lõike 5 mõte on tasakaalustada kahte olulist eesmärki. Ühelt poolt peab makseteenuse pakkujal olema tegelik võimalus pettuseriski korral sekkuda ning teha vajalikud maksejuhise kontrollitoimingud. Teiselt poolt ei tohi lisaturvameetmete rakendamine viia selleni, et maksete täitmine venib põhjendamatult või et makseteenuse kasutaja jääb määramata ajaks ebakindlasse olukorda. Seetõttu seob säte lubatava viivituse kestuse otseselt kontrolli eesmärgiga: viivitus on lubatav üksnes seni, kuni kestab põhjendatud kontroll ning ainult ulatuses, mis on selle kontrolli läbiviimiseks mõistlikult vajalik.

Eelnõus on loobutud rangest ajapiiri sätestamisest, sest kontrolli kestus ei pruugi kõikidel juhtudel olla sama. Mõnes olukorras piisab automaatsest kontrollist või lisakinnituse küsimisest, mille saab teha väga kiiresti, muus olukorras võib olla vaja teha täiendav riskihindamine või saada maksjalt kinnitus eri kanali kaudu.

Nimetatud tähtaeg kehtib ka välkmaksetele ning seda tuleb arvestada ka välkmaksete puhul maksejuhise täitmisel. Välkmaksete määruse kohaselt peab maksja makseteenuse pakkuja kohe pärast välkmaksejuhise kättesaamist kontrollima, kas makse töötlemise tingimused on täidetud ja kas vajalikud vahendid on olemas, ning saatma maksetehingu viivitamata saaja makseteenuse pakkujale. Saaja makseteenuse pakkuja peab omakorda tegema summa saaja kontol kättesaadavaks 10 sekundi jooksul alates sellest, kui maksja makseteenuse pakkuja välkmaksejuhise kätte sai. See näitab, et liidu seadusandja eesmärk on maksete, eriti välkmaksete, võimalikult kiire täitmine.

Teisalt ei saa turvakontrolli ajaline piirang muuta seda ebaefektiivseks. Välkmaksete määrus küll eeldab väga kiiret maksete täitmist, kuid samas säilib makseteenuse pakkuja kohustus ennetada pettusi ja rakendada turvanõudeid. Makseteenuste direktiiv ja komisjoni rakendusmäärus lähtuvad sellest, et maksete kõrgetasemeline turvalisus on makseteenuste toimimise üks põhielement. Kõnealune lõige 5 tasakaalustab neid kahte vastuolulist eesmärki: makseteenuse pakkuja võib maksejuhise kättesaamise edasi lükata, kuid ainult nii kaua, kui tal on tegelikult vaja tuvastada, kas tehing on õiguspärane; pärast seda tuleb maksejuhis saata viivitamata makse saaja makseteenuse pakkujale. Nii-öelda lubatav viivitus lõpeb siis, kui lõikes 4 nimetatud asjaolu väljaselgitamiseks mõistlikult vajalik aeg on möödunud. See võimaldab hiljem hinnata makseteenuse pakkuja tegevuse õiguspärasust ning vastutuse olemasolu.

Makseteenuste direktiivi järgi on makse täitmise tähtaeg seotud maksejuhise kättesaamise ajaga, artikli 78 lõike 1 kohaselt on maksejuhise kättesaamise aeg see hetk, mil maksja makseteenuse pakkuja maksejuhise kätte saab, ning artikli 83 lõike 1 kohaselt peab maksja makseteenuse pakkuja tagama, et pärast seda hetke kantakse maksesumma saaja makseteenuse pakkuja kontole hiljemalt järgmise tööpäeva lõpuks. Makseteenuste direktiiv näeb ette, et kui makseteenuse pakkuja keeldub õiguspäraselt maksejuhise täitmisest, loetakse selline maksejuhis täitmise tähtaegade mõttes kättesaamata maksejuhisena. Seega on maksejuhise "kättesaamise" mõiste otseselt seotud sellega, millal hakkavad kulgema täitmise tähtajad ning millal tekib makseteenuse pakkujal kohustus makset edasi töödelda.

Komisjoni rakendusmäärus lähtub tehingu riskipõhisest lähenemisest ning näeb ette, et makseteenuse pakkujatel peavad olema tehingute jälgimise mehhanismid, mis võimaldavad tuvastada autoriseerimata või pettuslike maksetehinguid. Need mehhanismid peavad põhinema maksetehingute analüüsil, arvestades seda, mis on konkreetse makseteenuse kasutaja puhul tavapärane, ning võtma arvesse vähemalt riskitegureid nagu maksja tavapäratud kulutused või käitumismuster; ebatavaline teave maksja seadme/tarkvara kasutamise kohta; pahavaraga nakatumine autentimismenetluse mis tahes seansi kestel ning makseteenuste osutamisega seoses teadaolev petuskeem (artikkel 2 lõige 2). Sama määruse põhjenduspunktis 14 on rõhutatud, et kui reaalajas riskianalüüs ei võimalda tehingut pidada madala riskiga tehinguks, tuleb makseteenuse pakkujal minna tagasi tugevdatud kontrolli juurde. Seega eeldab liidu õigus, et makseteenuse pakkuja teeb vajaduse korral lisakontrolle, kuid need kontrollid peavad olema seotud konkreetse riskihindamisega.

Eelnõu § 1 punktiga 2 VÕS-i lisatav 724[7] lõige 6 näeb ette, et maksja makseteenuse pakkujal on õigus keelduda maksejuhise täitmisest, kui pärast käesoleva paragrahvi lõikes 1 nimetatud lisaturvameetme rakendamist ei ole olnud objektiivselt võimalik kõrvaldada kahtlust, et maksejuhis on autoriseeritud andmete väärkasutamise, pettuse või maksjaga manipuleerimise teel. Sätte eesmärk on võimaldada makseteenuse pakkujal ennetada kahju tekkimist juba enne makse lõplikku täitmist.

Lõike 6 sõnastuses kasutatud kriteerium „objektiivselt võimalik" piirab makseteenuse pakkuja kaalutlusruumi ning välistab keeldumise pelgalt nn üldise riskihindamise või ebamäärase põhjenduse alusel. Keeldumine eeldab, et makseteenuse pakkuja on eelnevalt rakendanud

lisaturvameetmeid ning nende tulemusel ei ole kahtlust õnnestunud kõrvaldada. Seega peab keeldumise alus olema kontrollitav ja põhjendatav lähtuvalt faktiliselt olukorrast.

Eelnõu § 1 punktiga 2 VÕS-i lisatav 724^{7} lõige 7 näeb ette, et kui maksejuhise täitmine viibib käesoleva paragrahvi lõikes 1 sätestatud lisaturvameetmete rakendamise tõttu, hakkab käesoleva seaduse §-s 728 sätestatud maksejuhise täitmise tähtaeg kulgema alates maksejuhise kättesaamisest käesoleva paragrahvi lõikes 4 sätestatud tähenduses. Kõnealune lõige on seotud lõikega 4, sest juhul, kui maksejuhis loetakse kättesaaduks pärast lisaturvameetmete rakendamist, peab samas hetkest kulgema hakkama ka maksejuhise täitmise tähtaeg. Makseteenuste direktiivi artikkel 83 lähtub samuti sellest, et täitmise aeg arvutatakse alates artikli 78 tähenduses maksejuhise kättesaamise ajast. Kõnealune lõige tagab, et maksejuhise täitmise tähtaja arvestus järgib sama põhimõtet ka pettusekahtlusega juhtumite korral. Säte väldib olukorda, kus makseteenuse pakkuja satuks tähtaega rikkuma ajal, mil ta täidab seadusest tulenevat kohustust kohaldada lisaturvameetmeid.

Eelnõu § 1 punktiga 2 VÕS-i lisatav 724^{7} lõige 8 näeb ette, et kui käesoleva paragrahvi lõikes 1 nimetatud lisaturvameetmete rakendamise tulemusel täidetakse makse hilinemisega, kohaldatakse makse täitmisele käesoleva seaduse § 733^{3} lõigetes 4^{1} ja 4^{2} sätestatut.

VÕS § 733^{3} lõiked 4^{1} ja 4^{2} käsitlevad väärtuspäeva korrigeerimist hilinenud makse korral. Eelnõuga kõnealune VÕS-i lisatav § 724^{7} lõige 9 näeb ette õiguse lisaturvameetmete rakendamiseks ning asjaolude väljaselgitamisele, kas maksetehingu täitmiseks antud nõusolek on saadud andmete väärkasutamise, pettuse või maksja manipuleerimise teel, võib kuluda rohkem aega, kui on ette nähtud maksetehingu täitmiseks. Sellisel juhul tagab saaja makseteenuse pakkuja maksja makseteenuse pakkuja taotlusel, et saaja maksekonto krediteerimise väärtuspäevaks loetakse maksetehingu nõuetekohaseks täitmiseks määratud väärtuspäev. Seeläbi ei halvene maksja olukord, kuna kontole laekunud raha väärtuspäevaks loetakse algselt makse nõuetekohaseks täitmiseks ette nähtud kuupäev, isegi kui raha jõuab vastavale kontole tegelikult hiljem.

Kõnealune säte järgib juba kehtivat VÕS-i regulatsiooni hilinenud makse täitmise tagajärgede kohta ning ei loo selles osas eraldiseisvat regulatsiooni. Sätte eesmärk on tagada, et lisaturvameetmete rakendamine ei katkestaks kehtivas õiguses juba olemasolevat hilinenud makse täitmise tagajärgede regulatsiooni, vaid lähtuks samast loogikast. Tegemist ei ole eraldiseisva hilinenud täitmise režiimi loomisega, vaid olemasolevate tagajärgede kohaldamise täpsustamisega olukorras, kus maksetehingu täitmine viibib õiguspäraselt rakendatud lisaturvameetmete tõttu. VÕS § 733^{3} lõiked 4^{1} ja 4^{2} reguleerivad juba praegu, milline peab olema saaja maksekonto krediteerimise väärtuspäev juhul, kui makse täidetakse hilinemisega. Käesolev lõige tagab, et sama põhimõte kohaldub ka siis, kui hilinemise põhjus seisneb makseteenuse pakkuja poolt pettuskahtluse kontrollimiseks rakendatud lisaturvameetmetes. Sellega välditakse olukorda, kus makse formaalselt hilineb, kuid hilinemise mõju saaja konto väärtuspäeva osas jääks reguleerimata. Lahendus on kooskõlas ka makseteenuste direktiivis sätestatud hilinenud täitmise regulatsiooniga, mille kohaselt tuleb hilinenud makse korral tagada, et saaja konto krediteerimise päev ei oleks hilisem päevast, mil tehing oleks pidanud

olema õigesti täidetud. Makseteenuste direktiivi artikkel 89 näeb selle põhimõtte sõnaselgelt ette.

Kui maksejuhise on algatanud maksja, kohaldub VÕS § 733^3 lõige 4^1. Selle järgi tagab saaja makseteenuse pakkuja maksja makseteenuse pakkuja taotlusel, et saaja maksekonto krediteerimise väärtuspäevaks loetakse maksetehingu nõuetekohaseks täitmiseks määratud väärtuspäev. Seega tagab lõige 8, et lisaturvameetmete tõttu tekkinud viivitus ei muudaks hilinenud makse tagajärgede käsitlust võrreldes muude hilinenud maksetega. Maksja algatatud makse puhul näiteks olukord, kus isik teeb internetipangas ülekande teisele isikule. Tegemist on maksja algatatud maksega ning kohaldub VÕS § 733^3 lõige 4^1.

Kui makse on algatatud saaja poolt või tema kaudu, kohaldub VÕS § 733^3 lõige 4^2. Selle järgi loetakse saaja maksekonto krediteerimise väärtuspäevaks samuti maksetehingu nõuetekohaseks täitmiseks määratud väärtuspäev. Kõnealusel juhul näiteks kui makse saaja algatatud makse korral võetakse isiku kontolt otsekorralduse alusel makse kommunaalteenuse osutajale. Sellisel juhul kohaldub VÕS § 733^3 lõige 4^2.

Eelnõu § 1 punktiga 2 VÕS-i lisatav 724^7 lõige 9 näeb ette, et makseteenuse leping võib sisaldada tingimust, mille kohaselt maksja ei või nõuda lisaturvameetmete rakendamiseks maksejuhise kättesaamise edasi lükkamise korral maksja makseteenuse pakkujalt kahju hüvitamist. Hüvitist ei või nõuda tingimusel, et nimetatud turvameetmeid rakendatakse ebamõistliku viivituseta ning rakendamise aluseks on objektiivselt põhjendatud kahtlus, et maksejuhise autoriseerimiseks antud nõusolek on saadud andmete väärkasutamise, pettuse või maksjaga manipuleerimise teel. See lepingu tingimus ei välista ega piira maksja muu nõude esitamist muul alusel.

Kui makseteenuse pakkuja rakendab maksetehingu kontrollimiseks lisaturvameetmeid võib selle peale kuluda rohkem aega, kui on ette nähtud maksetehingu täitmiseks. Alati ei pruugi lisaturvameetmete rakendamise tulemuseks olla maksejuhise täitmisest keeldumine, kuna kontrolli tulemusel selgub, et tegemist ei ole pettusega ning isik on andnud nõusoleku maksetehingu täitmiseks. Juhul, kui makseteenuse pakkuja on turvameetme täiendava rakendamise läbi viinud õiguspäraselt vastavalt eelnõuga VÕS-i lisatava § 733^9 lõike 3 tingimustele, ei vastuta makseteenuse pakkuja kahju eest, mis on tekkinud tehingu hilinenud täitmise tõttu.

Sätte eesmärk on tagada, et makseteenuse pakkuja ei oleks kohustatud kandma kahju seetõttu, et ta tegutses maksja kaitseks ja tema pettuseohvriks langemise ärahoidmiseks. Kui makseteenuse pakkuja rakendab põhjendatud kahtluse korral viivitamata lisaturvameetmeid on selle eesmärgiks kliendi kaitse. Sellises olukorras oleks ebamõistlik panna makseteenuse pakkujale automaatne kahju hüvitamise kohustus pelgalt ajutise viivituse tõttu. Säte tasakaalustab maksja huvi makse kiire täitmise vastu ning maksesüsteemi turvalisuse tagamist.

Kõnealuse lõikes 9 vastutuse piiramine on sõnastatud kitsalt ja tingimuslikult. Vastutus ei ole välistatud igas olukorras, vaid eeldab kumulatiivselt, et lisaturvameetmeid rakendatakse ebamõistliku viivituseta ning nende aluseks on objektiivselt põhjendatud kahtlus. Lisaks on

sättes selgelt toodud, et see lepingu tingimus ei välista ega piira maksja muu nõude esitamist muul alusel. Seega ei kõrvalda muudatus makseteenuse pakkuja üldist vastutust ega kahjusta maksja õigust tugineda muudele õiguskaitsevahenditele, kui makseteenuse pakkuja on tegutsenud õigusvastaselt, ebaproportsionaalselt või põhjendamatult. Selline lahendus on kooskõlas makseteenuste direktiivi üldise vastutuse loogikaga, mille kohaselt makseteenuse pakkuja vastutus makse mittetäitmise, puuduliku täitmise või hilinenud täitmise eest on reguleeritud, kuid direktiiv ei välista, et riigisisene õigus näeb ette riigisisese vastutuse. Kõnealune säte ei muuda üldiselt makseteenuste direktiivi kahju hüvitamise loogikat, kus makseteenuse pakkuja vastutab autoriseerimata kahju hüvitamise eest. Kõnealust põhimõtet ei muudeta, sest muudatuse näol on tegemist võimaliku kahjuga, mis on tekkinud autoriseeritud maksejuhise kontrollimisel ja maksejuhise hilisema täitmise korral. On oluline rõhutada, et käesolev muudatus annab makseteenuse pakkujatele õiguse keelduda autoriseeritud maksejuhise täitmisest, mis on erinev üldisest loogikast, et makseteenuse pakkuja ei või keelduda autoriseeritud maksejuhise täitmisest. Ehk et olukorras, kus makseteenuse pakkuja ei ole tõkestanud maksejuhise täitmist, mille isik on ise manipuleerimise teel PIN 2-ga kinnitanud, siis tegemist on ikkagi autoriseeritud maksejuhisega ning sellises olukorras ei kohaldu makseteenuse pakkuja vastutus autoriseerimata makse puhul kahju hüvitamiseks.

Eelnõu §-ga 2 muudetakse KAS-i.

Eelnõu § 2 punktiga 1 täiendatakse KAS §-i 88 lõike 3 punkti 1 pärast tekstiosa „käesolevas paragrahvis“ tekstiosaga „või käesoleva seaduse §-s § 89^4“.

KAS § 88 lõige 3 punkt 1 sätestab krediidiasutuse õiguse avaldada pangasaladust kolmandale isikule, kui krediidiasutuse õigus või kohustus avaldada pangasaladust tuleneb käesolevas paragrahvis sätestatust. See annab ammendava loetelu, mille kohaselt on krediidiasutusel õigus avaldada pangasaladust kolmandale isikule üksnes juhul, kui selline õigus või kohustus tuleneb KAS § 88 muudest sätetest, ehk muudel alustel ei ole võimalik pangasaladust avaldada. Eeltoodust tulenevalt sätestatakse KAS §-i 88 ka võimalus avaldada pangasaladust eelnõuga loodava § 89^4 alusel.

Eelnõu § 2 punktiga 2 täiendatakse KAS-i 7. peatüki 3. jaotist §-ga 89^4.

KAS-i lisatav uus paragrahv annab krediidiasutustele selged õiguslikud alused avaldada andmeid ja teavet pettuste avastamiseks ja väljaselgitamiseks juhul, kui krediidiasutusel on objektiivselt põhjendatud kahtlus, et klient või maksetehing võib olla seotud pettusega. Kehtiv KAS § 88 reguleerib iseenesest juba pangasaladuse avaldamist, mh näeb ette, et millistel tingimustel ja kuidas võib pangasaladust edastada nii PPA-le kui RIA-le. Samas kehtiv KAS § 88 ei näe otseselt ette krediidiasutustele õigust jagada pettuse kahtluse korral andmeid nii teiste krediidiasutustega, makseasutuste ja e-raha asutustega kui ka teiste ametiasutustega. Uue KAS §-s 89^4 ettenähtud andmete puhul ei pruugi aga tingimata tegemist olla pangasaladusega (nt tegemist võib olla koondandmetega või muude sarnaste andmetega, mille põhjal ei saa kindlaks teha üksikkliendi andmeid). Tulenevalt eeltoodust on otsustatud, et ei täiendata kehtivat KAS §-i 88, vaid konstrueeritakse KASi vastav uus § 89^4. Lisaks tuleb suure tõenäosusega vastav

normistik kehtetuks tunnistada, kui tulevikus hakkab kehtima eespool nimetatud EL makseteenuste määrus (ehk ka õigustehniliselt on lihtsam kustuda eraldiseisvat paragrahvi).

KAS uue §-i 89[4] lõike 1 kohaselt antakse krediidiasutusele õigus avaldada erinevat teavet, mh pangasaladust teisele krediidiasutusele, makseasutusele ja e-raha asutusele ning PPA-le maksetehingutega seotud pettuste avastamiseks ja väljaselgitamiseks juhul, kui krediidiasutusel on objektiivselt põhjendatud kahtlus, et klient või maksetehing võib olla seotud pettusega. Pettuste tõkestamisel on oluline kiirus ning koostöö, et oleks võimalik operatiivselt sekkuda. Kehtiva KAS-i § 88 lõike 5 punkt 2 võimaldab pangasaladuse avaldamist uurimisasutusele üksnes kriminaalmenetluse raames. Seega on politseil küll võimalik saada pettuste uurimisel informatsiooni, kuid see on piiratud, sest andmete avaldamine eeldab kriminaalmenetluse algatamist. **Eelnõuga kavandatav paragrahv loob õigusliku aluse, mis võimaldab krediidiasutusel objektiivselt põhjendatud pettuse kahtluse korral edastada andmeid enne kriminaalmenetluse algatamist.** See võimaldab kiiremat reageerimist ja kahju tekkimist olukordades, kus menetluse alustamine võib toimuda alles pärast esmast juhtumi analüüsi ning pettuse ärahoidmise vaatest seega liiga hilja.

Antud juhul nähakse ette andmete jagamine krediidiasutusele õigusena, kui selliste andmete jagamine osutub krediidiasutuse hinnangul vajalikuks. Pangasaladuse avaldamine ei ole lubatud iga kahtluse korral, vaid juhul, kui selleks on objektiivselt põhjendatud pettuse kahtlus, näiteks:

- isik võib olla seotud pettuse toimepanemisega või konkreetne maksetehing võib olla seotud pettusega, ning see peab tuginema kontrollitavatele asjaoludele;
- esinevad pettustele iseloomulikud tehingumustrid, kus lühikese aja jooksul tehakse mitmeid uutele saajatele suurtes summades ülekandeid ning samuti tehnilised andmed, kus seade või sessioon kattub varem tuvastatud pettusega.

Uue paragrahvi § 89[4] lõige 2 näeb ette, millist liiki andmete avaldamine lubatud on. Pettuseid ei pruugi olla võimalik avastada nn üksiku „andmetüki" põhjal, vaid praktikas on vajalik andmete kogum, mille põhjal saab omavahel siduda pettuse kahtlusega isikud, kontod, seadmed, sessioonid jne.

Antud lõike punktis 1 nimetatud andmed kliendi kohta on isiku tuvastamiseks vajalikud unikaalsed identifikaatorid, mille abil saab kindlaks teha millise isikuga on tegemist. Nendeks võivad olla näiteks kliendi-ID, isikukood või kontonumber. Näiteks krediidiasutus A tuvastab, et kliendi kontolt tehakse ebaharilikke makseid erinevatele saajatele ning on alus kahtlustada pettuse toimepanemist, siis on võimalik teavitada krediidiasutust B, kellele makseid tehakse ning edastada isiku andmed, et saaks kontrollida, kas saaja või tema maksekonto võib olla seotud pettusega.

Punkti 2 kohaselt saab edastada andmeid makse saaja ja maksekonto kohta, mis on vajalikud saaja identifitseerimiseks, et tuvastada pettuse ahelas saaja pool. Näiteks olukord, kus mitmed isikud teevad ebaharilikke makseid ühele makse saajale. Sel juhul saab krediidiasutus edastada makse saaja krediidiasutusele kõnealused andmed, et teine krediidiasutus saaks hinnata, kas tegemist võib olla nn rahamuula maksekontoga. See aitab tuvastada erinevate petta saanud

isikute maksed sama makse saaja krediidiasutusele ning takistada raha liikumist rahamuulade maksekontode vahel.

Punkti 3 kohaselt saab edastada andmeid maksetehingute kohta, mis on konkreetse maksetehingu tunnused, näiteks tehingu ID. Nimetatud andmed maksetehingu kohta hõlmavad üksnes konkreetse pettusekahtlusega seotud makse asjaolusid, mis on vajalikud pettuse avastamiseks ja väljaselgitamiseks. Nende andmete all ei peeta silmas kliendi konto väljavõtet ega muud terviklikku ülevaadet kliendi maksekäitumisest, selliste andmete väljastamine ei ole lubatud. Konto väljavõtte avaldamine ületaks kõnealuse regulatsiooni eesmärgi ning ei oleks kooskõlas andmete minimaalsuse põhimõttega. Seetõttu on lubatud avaldada üksnes selliseid konkreetse maksetehingu andmeid, nagu tehingu aeg, tehingu liik, kasutatud kanal või muud asjaolud, millel on vahetu tähendus pettusekahtluse kontrollimiseks.

Punktis 4 nimetatud andmed kasutatud seadme, makseinstrumendi või turvaelementide kohta on vajalikud selleks, et maksetehinguga seotud pettusi oleks võimalik avastada ja välja selgitada ka olukorras, kus pettusekahtlus ei ilmne üksnes kliendi, saaja või konkreetse makseandmete pinnalt, vaid eeskätt sellest, millise tehnilise vahendi või autentimisviisiga tehing tehti. Pettused võivad avalduda näiteks olukordades, kus kasutatakse sama seadet, sama autentimisvahendit või samu turvaelemente mitme kahtlase tehingu tegemisel. Selliste andmete võrdlemine võimaldab tuvastada pettusmustreid, seostada omavahel eri juhtumeid ning hinnata, kas tegemist võib olla andmete väärkasutamise, identiteedi kuritarvitamise või muu pettusliku skeemiga.

Kasutatud seadme, makseinstrumendi või turvaelementide kohta käiv teave ei kattu täielikult ei kliendiandmete, makse saaja ja maksekonto andmete ega ka üksnes maksetehingu andmetega. Kliendi või konto tuvastamine ei näita veel, kuidas tehing tehniliselt tehti või milliseid autentimisvahendeid kasutati. Just seadme, makseinstrumendi või turvaelementide kohta käiv info võib osutada, et näiliselt erinevad tehingud on tegelikult omavahel seotud, näiteks kui need on tehtud sama seadme või sama maksevahendi abil. Selline teave võib olla määrava tähtsusega, et eristada kliendi tavapärast maksekäitumist olukorrast, kus maksevahendit või autentimisvahendeid on väärkasutatud.

Andmeteks on näiteks seadme- ja sessiooniandmed ning muud pettuse tuvastamist võimaldavad tehnilised andmed, mille alusel saab tuvastada, kas makse algatamise keskkond on ebatavaline, näiteks seadme-ID, brauser, IP-aadress. See aitab tuvastada, kas erinevate isikute kontodelt algatatakse makseid sama seadmega või samalt IP-aadressilt, kuigi isikud on erinevates piirkondades. Nende andmete jagamine aitab tuvastada pettuse toimepanemist laiemalt erinevate krediidiasutuste üleselt, mida üks krediidiasutus oma andmete pinnalt ei pruugi tuvastada.

Punktiga 5 nähakse ette andmete ja teabe jagamine maksetehinguga seotud pettuse või muu süüteo tunnustele vastava teo kohta. See on andmed ja teave mille järgi on näha, et tegemist võib olla pettus või muu süüteoga. Tegemist ei pea olema juba kinnitust leidnud pettusjuhtumiga, vaid pigem andmete ja tunnustega, mis osutavad võimalikele rikkumise tunnustele. Siia võivad kuuluda näiteks andmed ebatavalise käitumismustri kohta, vastuolud

makse algatamise tavapärases loogikas, andmed selle kohta, et kasutatud on võõrast või ootamatut seadet, turvaelemente on kasutatud ebatavapärasel viisil, või muud asjaolud, mis eraldi või kogumis loovad objektiivselt põhjendatud kahtluse, et tehing võib olla seotud pettuse või muu süüteoga. See on suunatud ennekõike süüteotunnuste, riskinäitajate ja kahtlust toetavate asjaolude kirjeldamisele. Selle punkti eesmärk on võimaldada vahetada sellist teavet, mis aitab pettust või muud võimalikku süütegu tuvastada, selle olemasolu kontrollida ja hinnata, kas on alust võtta kasutusele täiendavaid meetmeid.

Erinevalt punktist 6 ei ole käesoleva punkti 5 puhul tegemist juba toimunud pettusejuhtumiga. Pettuste avastamise ja väljaselgitamise seisukohast on oluline võimalus vahetada ka sellist teavet, mis ei kirjelda veel lõplikult tuvastatud pettust, kuid mis võib viidata pettuse või muu süüteo tunnustele ning aidata ennetada kahju tekkimist või levikut. Samal ajal on vajalik eraldi nimetada ka juba toime pandud pettuse teel tehtud tehingud ja pettusekatsed, sest nende kohta kogutav ja vahetatav teave on tavaliselt konkreetsem, detailsem ja otsesemalt seotud konkreetse juhtumi lahendamisega.

Punktiga 6 nähakse ette andmete ja teabe jagamine pettuse teel tehtud tehingute või pettusekatsete ja nende asjaolude kohta. Need on andmed ja teave toime pandud või toime panna üritatud pettusjuhtumi ning selle konkreetsete asjaolude kohta. Need on nn pettuseindikaatorid, mis kirjeldavad petuskeemi toimimist, nagu näiteks tehingu ajastus ja korduvad summad ning mitme isiku samasugused käitumisjooned. See aitab pettuste toimepanemist avastada näiteks olukorras, kus mitmed kliendid saavad samal päeval panga nimel petukõnesid, siis on võimalik jagada pettusekatsete mustreid teiste krediidiasutustega ning tuvastada nn saripettuse toimepanemine võimalikult vara ka teistel krediidiasutustel ning seeläbi kahjusid vähendada.

Eeltoodu võib olla tuvastatud manipuleerimise tehnikad või muud pettuslikud võtted. Pettuse toimepanijate nn töövõtted on näiteks krediidiasutuse töötajana esinemise legend, kiire tegutsemise surve kindlate pettuse liikide puhul, pahavara allalaadimise juhendamine jne. Näiteks krediidiasutusele teavitavad mitmed isikud samasuguse sisuga krediidiasutuse töötajana esinenud pettuslikust kõnest.

Uue § 89[4] lõikega 3 nähakse krediidiasutusele ette õigus avaldada pangasaladust ka RIA-le. Kehtiv KAS § 88 lg 4[3] annab krediidiasutusele õiguse avaldada pangasaladust RIA-le küberturvalisuse seaduses sätestatud riikliku järelevalve tegemisel.

RIA on Eesti küberturvalisuse keskus, mis tegeleb avaliku sektori ja kriitilise infrastruktuuri küberturvalisusega ning on võrgu- ja infosüsteemide turbe direktiivi (NIS)[13] mõistes küberturvalisuse pädev asutus ja kontaktpunkt.

Nagu eespool juba märgitud, siis uue paragrahvi kohaselt RIA-le avaldatatavad andmed ei pruugi kõik kvalifitseeruda pangasaladuseks. Lisaks arvestades RIA ülesannet on temale avaldada lubatud andmete koosseis lõike 3 näol kitsam (kui lõikes 1 PPA puhul), piirdudes üldisemalt andmetega pettuse teel tehtud tehingute või pettusekatsete ja nende asjaolude kohta

[13] https://eur-lex.europa.eu/eli/dir/2022/2555/oj/est

ning maksetehinguga seotud pettuse või muu süüteo tunnustele vastava teo tuvastamist võimaldavaid andmeid. RIA-le ei avaldata andmeid ja teavet 1) kliendi tuvastamiseks; 2) makse saaja ja maksekonto kohta ning 3) maksetehingute kohta, sealhulgas muid makseandmeid.

Lõikes 3 nähakse ette, et RIA-le saab andmeid jagada küberturvalisuse seaduse (edaspidi *KüTS*) § 5 lõige 3 punkt 3 alusel. See punkt sätestab, et RIA täidab EL direktiivi (EL) 2022/2555 artikli 10 lõikes 1 nimetatud küberintsidentide käsitlemise üksuse ülesanded. Eelnimetatud direktiivi artikli lõige 2 viitab ülesannetele, mis on sätestatud direktiivi artikli 11 lõikes 3. Näiteks on artikli 11 lõike 3 kohaselt vastavateks ülesanneteks:
- tagada küberohtude, nõrkuste ja intsidentide kohta varajaste hoiatuste, hoiatuste ja teadete edastamine ning teabe levitamine asjaomastele elutähtsatele ja olulistele üksustele ning pädevatele asutustele ning muudele asjaomastele sidusrühmadele, võimaluse korral reaalajalähedaselt;
- lahendada intsidente ning, kui see on kohaldatav, abistada asjaomaseid elutähtsaid ja olulisi üksusi.

Kuna kehtiv KAS annab võimaluse avaldada pangasaladust üksnes riikliku järelevalve tegemisel, ei ole RIA-l võimalik väljaspool seda sekkuda küberturvalisust ohustavatele olukordadele. Majandus- ja kommunikatsiooniministeeriumi 25. aprilli 2011. aasta määruse nr 28 „Riigi Infosüsteemi Ameti põhimäärus“ § 8 lõike 4 punkti 3 kohaselt täidab küberturvalisuse valdkonnas amet küberturvalisuse seaduse § 5 tähenduses pädeva asutuse, ühtse kontaktpunkti, ulatuslike küberintsidentide ja kriiside ohjamise eest vastutava pädeva asutuse, küberintsidentide käsitlemise üksuse ja turvahaavatavuse koordineeritult avaldamise koordinaatori ülesandeid ning koordineerib küberintsidentide käsitlemist. Sama paragrahvi lõige 4 punkt 4 kohaselt korraldab küberturvalisuse amet küberturvalisust ohustavate riskide seiret, analüüsi ja ohtudest teavitamist. KAS-i lisatav uus paragrahv annab võimaluse avaldada andmeid ja teavet ka olukordades, mis on väljaspool riikliku järelevalve menetlust. See annab võimaluse sekkuda küberintsidentide puhul operatiivselt. Andmete avaldamise korral üksnes järelevalve menetluse raames jõuab teave RIA-le liiga hilja ning see takistab RIA-l sekkuda intsidentidesse reaalajas.

RIA töötleb andmeid avalikes huvides oleva ülesande täitmiseks, milleks on küberintsidentide käsitlemine ja küberturvalisust ohustavate riskide ennetamine. Maksetehingutega seotud pettused on sageli seotud infosüsteemide ründamise, autentimisvahendite kuritarvitamise või muu küberohuga ning võivad kujutada endast osa laiemast või koordineeritud küberintsidendist. Selliste juhtumite puhul ei ole tegemist üksnes isiku varakahjuga, vaid riskiga maksesüsteemide ja infosüsteemide turvalisusele laiemalt. RIA kui küberturvalisuse pädev asutus vajab teavet pettuse olemuse, ründeviiside ja kasutatud tehniliste vahendite kohta, et tuvastada rünnakumustreid, hinnata riske ning vajaduse korral teavitada teisi teenuseosutajaid ja koordineerida reageerimist.

Kokkuvõttes ei avaldata RIA-le andmeid kliendi tuvastamiseks, makse saaja ega maksekonto andmeid ega muid makseandmeid. Avaldada on lubatud üksnes pettuse teel tehtud tehingute või pettusekatsete asjaolusid ning maksetehinguga seotud pettuse või muu süüteo tunnustele

vastava teo tuvastamist võimaldavaid andmeid. Seega on andmete avaldamine suunatud eeskätt tehnilise ja mustripõhise analüüsi võimaldamisele, mitte üksikisikute tuvastamisele.

Uue § 89[4] lõike 4 kohaselt on krediidiasutusel õigus avaldada e-identimise ja e-tehingute usaldusteenuste seaduse tähenduses e-allkirjastamist võimaldavale usaldusteenuse osutajale käesoleva paragrahvi lõikes 1 nimetatud eesmärgil usaldusteenuse kasutaja, seadme- ja sessiooniandmed ning kasutaja elektroonilise side võrgu identifikaatori andmed.

Nimetatud andmete avaldamise vajadus seisneb selles, et pettusekahtluse korral ei pruugi krediidiasutusel olla võimalik üksnes enda valduses oleva info põhjal kontrollida, kas e-allkirjastamine või muu usaldusteenuse kasutamine toimus tegelikult selle kasutaja enda poolt või kasutati seda pettuslikult. Usaldusteenuse osutaja on see osapool, kellel on info e-allkirjastamise või muu usaldusteenuse kasutamise tehniliste andmete kohta. Seetõttu võib pettuse avastamiseks või väljaselgitamiseks olla vajalik, et krediidiasutus saaks konkreetse juhtumi puhul avaldada usaldusteenuse osutajale piiratud hulka identifitseerivaid ja tehnilisi andmeid. Andmete avaldamine on ühepoolne ning selle põhjal saab usaldusteenuse osutaja kontrollida, kas tema teenust on konkreetse pettusekahtlusega juhtumi raames kasutatud pettuse teel, ning rakendada vajaduse korral enda pädevuses olevaid kaitsemeetmeid, näiteks teenuse kasutamist ajutiselt piirata.

Ilma kõnealuste andmeteta ei oleks võimalik usaldusteenuse pakkujal kontrollida, kas vaidlusalune allkirjastamistoiming või muu usaldusteenuse kasutamine toimus sama isiku nimel, kelle maksetehingu suhtes tekkis pettusekahtlus. Seadme- ja sessiooniandmed on vajalikud selleks, et võrrelda, kas konkreetne teenuse kasutus langes kokku usaldusteenuse osutaja süsteemides registreeritud tehniliste tunnustega, näiteks kas kasutati sama seadet, sama sessiooni või sarnast tehnilist keskkonda. Kasutaja elektroonilise side võrgu identifikaatori andmed aitavad kontrollida, kas vaidlusalune kasutamine toimus samast võrgukeskkonnast või sama tehnilise lähtepunkti kaudu, mis seostub ka võimaliku pettusliku maksetehinguga. Säte eesmärk on lubada andmete avaldamist üksnes konkreetse pettusekahtlusega juhtumi kontrollimiseks ja ulatuses, mis võimaldab konkreetset juhtumit kontrollida.

Uue § 89[4] lõikega 5 nähakse ette, et andmete ja teabe avaldamisel ei ole lubatud avaldada eriliiki isikuandmeid. Andmete ja teabe avaldamise eesmärk on maksepettuse avastamine ja väljaselgitamine ning selle eesmärgi saavutamiseks ei ole eriliiki isikuandmete avaldamine üldjuhul vajalik. See suurendaks põhiõiguste riivet ja oleks vastuolus andmete minimaalsuse ning ebaproportsionaalne.

Eelnõu §-ga 3 muudetakse MERAS-t.

Eelnõu §-ga 3 täiendatakse MERAS §-i 63[3] lõigetega 2 ja 3. Lõike 2 kohaselt on makseteenuse pakkujatele õigus avaldada andmeid ja teavet teisele makseasutusele ja e-raha asutusele, krediidiasutusele, PPA-le ning RIA-le maksepettuste avastamiseks ja väljaselgitamiseks krediidiasutuste seaduse §-is 89[4] sätestatud tingimustel. Kuna makseteenuseid osutavad ka makseasutused ja e-raha asutused, antakse ka neile krediidiasutusega samasugune õigus andmeid avaldada. Vastasel juhul jääb osa

teenusepakkujaid pettuste ennetustegevusest väljapoole just puuduva info tõttu. Andmete avaldamise eesmärk ja koosseis on sama nagu krediidiasutustel.

Lõike 3 kohaselt on makseteenuse pakkujal on õigus avaldada E-identimise ja e-tehingute usaldusteenuste seaduse tähenduses e-allkirjastamist võimaldavale usaldusteenuse osutajale krediidiasutuste seaduse § 89^4 lõikes 1 nimetatud eesmärgil usaldusteenuse kasutaja isikukood, seadme- ja sessiooniandmed ning kasutaja elektroonilise side võrgu identifikaatori andmed. Ka siin on andmete avaldamise eesmärk ja koosseis sama nagu krediidiasutustel.

4. Eelnõu vastavus Eesti Vabariigi põhiseadusele

4.1 Andmete avaldamise ja töötlemise vastavus põhiseadusele

Isikute põhiõigus võib piirata ainult kooskõlas põhiseadusega. Isikute põhiõigustesse sekkumine on põhiseaduspärane, kui see on formaalselt ja materiaalselt põhiseadusega kooskõlas. Materiaalne põhiseaduspärasus tähendab, et põhiõiguse riive on kehtestatud (a) legitiimselt ehk põhiseadusega lubatava eesmärgi saavutamiseks ning (b) on selle legitiimse eesmärgi saavutamiseks proportsionaalne. Materiaalset põhiseaduspärasust kontrollitakse järgmise skeemi alusel: esmalt tehakse kindlaks põhiõiguse esemeline ja isikuline kaitseala ning seejärel kirjeldatakse, kuidas õigusakt põhiõigust riivab. Tuleb hinnata, kas riivel on legitiimne eesmärk ning teostada proportsionaalsuse test - kas riive on legitiimse eesmärgi saavutamiseks sobiv, vajalik ja mõõdukas. Andmete kogumine füüsiliste ja juriidiliste kohta riivab eelkõige õigust eraelu puutumatusele (PS § 26) ja õigust informatsioonilisele enesemääramisele (PS § 19). Õigus eraelu puutumatusele PS § 26 kaitseb isiku õigust eraelu puutumatusele ning keelab riigil sellesse sekkuda muul juhul, kui seaduses sätestatud juhtudel ja korras tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks. Õigus informatsioonilisele enesemääramisele Samuti riivab isikuandmete töötlemine PS §-ist 19 tulenevat isiku informatsioonilist enesemääramist. Informatsiooniline enesemääramine tähendab, et igaühel on õigus ise otsustada, kas ja kui palju tema kohta andmeid kogutakse ja salvestatakse.

Andmete töötlemise eesmärk on maksetehingutega seotud pettuste avastamine ja väljaselgitamine ning kaitsta seeläbi makseteenuse kasutajaid varalise kahju eest. Isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkti e kohaselt on isikuandmete töötlemine seaduslik juhul, kui isikuandmete töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks. Pettused makseteenuste valdkonnas põhjustavad klientidele varalist kahju ning kahjustavad usaldust maksesüsteemi kui terviku vastu. Pettuste ärahoidmine on ka üheks makseteenuste direktiivi eesmärgiks ning artikli 94 lõike 1 kohaselt liikmesriigid lubavad maksesüsteemidel ja makseteenuse pakkujatel töödelda isikuandmeid, kui see on vajalik maksepettuste ärahoidmise, uurimise ja avastamise tagamiseks.

Eelnõu annab makseteenuse pakkujatele õiguse avaldada pettusekahtluse korral piiratud adressaatide ringile andmeid kliendi, makse saaja, maksekonto, maksetehingu, pettuse või muu süüteo tunnustele vastava teo, kasutatud seadme, makseinstrumendi või turvaelementide ning pettuse teel tehtud tehingute või pettusekatsete ja nende asjaolude kohta. Kuna riive ei ole kõigi

andmekategooriate puhul ühesugune, tuleb põhiseaduspärasust hinnata erinevate andmekategooriate kaupa, mis võimaldab hinnata, kas iga konkreetse andmeliigi avaldamine on eesmärgi saavutamiseks sobiv, vajalik ja mõõdukas.

1. Kliendi kohta käivate andmete avaldamine

Kliendiandmete avaldamine riivab eraelu puutumatust ja informatsioonilist enesemääramist, sest tegemist on isikut tuvastada võimaldava teabega. Kliendiandmete avaldamise legitiimne eesmärk on maksepettuste avastamine ja väljaselgitamine ning seeläbi teiste isikute varaliste õiguste kaitse ja kuritegude tõkestamine. Nende andmete avaldamine on eesmärgi saavutamiseks sobiv, sest ilma kliendi identiteeti siduva teabeta ei ole võimalik kontrollida, kas sama isik on seotud ka teiste võimalike pettuse juhtumitega teiste makseteenuse pakkujate juures või PPA menetlustes. Pettustega seotud teave on praktikas sageli killustunud erinevate krediidiasutuste, teiste makseteenuse pakkujate ja ametite vahel ning kliendi andmete õigeaegne jagamine võimaldab kontrollida, kas ta on seotud teiste samalaadsete juhtumisega. Andmeid avaldatakse määratletud isikute ringile ning konkreetsel eesmärgil.

Meede on ka vajalik, sest vähem riivavam lahendus, näiteks pseudonümiseeritud või anonüümseks muudetud andmed ei võimaldaks konkreetset isikut tuvastada ega seostada erinevates süsteemides ilmnenud pettusekahtlustega. Mõõdukuse seisukohalt kaalub riivega saavutatav hüve võimaliku kahju üles, kui avaldatakse üksnes konkreetse juhtumi lahendamiseks vajalikud kliendiandmed, mitte kogu kliendiprofiil või kliendisuhte ajalugu.

2. Makse saaja ja maksekonto kohta käivate andmete avaldamine

Ka makse saaja ja maksekonto kohta andmete avaldamise legitiimne eesmärk on maksepettuste avastamine ja väljaselgitamine ning seeläbi teiste isikute varaliste õiguste kaitse ja kuritegude tõkestamine. Nende andmete avaldamine on eesmärgi saavutamiseks sobiv, sest pettuse teel saadud rahalised vahendid kantakse konkreetsele makse saajale ja maksekontole ning pettuste avastamiseks ja väljaselgitamiseks on vaja tuvastada, kuhu rahalised vahendid kanti ja samuti kas sama konto või saaja on seotud teiste sarnaste juhtumisega. Meede on vajalik, sest ilma andmeteta makse saaja ja maksekonto kohta ei oleks teistel makseteenuse pakkujatel ega PPA-l võimalik konkreetset maksetehingut kontrollida ega võtta vajaduse korral samme kahju vältimiseks või selle suurenemiseks. Oluline on, et maksekonto väljavõtte avaldamine on keelatud ehk et ei ole võimalik teha selle põhjal järeldusi nt isiku finantssuhete, varalise seisu või üldiselt maksekäitumise kohta. Seetõttu saab meedet pidada mõõdukaks, kuna teavet avaldatakse üksnes konkreetse juhtumi kohta ning ulatuses, mis on vältimatult vajalik pettuse avastamiseks või väljaselgitamiseks. Ainult makseteenuse pakkuja sisemisest kontrollist ei pruugi piisata, kui pettus hõlmab teise makseteenuse pakkujate kontot ning teise makseteenuse pakkuja kaudu tehtud tehinguid, mis ilmnevad alles eri juhtumite omavahelisel võrdlemisel.

3. Maksetehingu kohta käivate andmete avaldamine

Kõnealuste andmete avaldamine on eesmärgi saavutamiseks sobiv, sest pettuse avastamine ei sõltu üksnes osapoolte identifitseerimisest, vaid ka võimaliku pettusliku maksetehingu

tunnustest. Nimetatud andmed maksetehingu kohta hõlmavad üksnes konkreetse pettusekahtlusega seotud makse asjaolusid, mis on vajalikud pettuse avastamiseks ja väljaselgitamiseks. Nende andmete all ei peeta silmas kliendi konto väljavõtet ega muud terviklikku ülevaadet kliendi maksekäitumisest, selliste andmete väljastamine ei ole lubatud. Näiteks võib maksetehingu summa, ajastus ning selle unikaalne tunnus maksetehingu üheselt kindlaks teha. Vähem õigusi riivama meetmena näiteks üksnes anonümiseeritud või statistilise info jagamine ei võimaldaks konkreetse pettuskahtluse korral tuvastada asjaosalisi ning siduda konkreetseid tehinguid ja kontosid ega võtta viivitamata tarvitusele abinõusid konkreetse kahju ärahoidmiseks. Samuti ei täidaks eesmärki see, et andmeid võiks edastada alles pärast süüteomenetluse alustamist, sest pettuste puhul on andmete kiirel liikumisel otsene tähtsus kahju tekkimise või selle suurenemise ärahoidmisel. Seetõttu on kavandatud piiratud andmevahetuse õigus eesmärgi saavutamiseks vajalik.

4. Andmed kasutatud seadme, makseinstrumendi või turvaelementide kohta

Meede on eesmärgi saavutamiseks sobiv, sest maksepettused on tihti seotud korduvate tehniliste tunnustega ning sama seade, makseinstrument või autentimisviis võib siduda näiliselt eraldiseisvaid juhtumeid. Kasutatud seadme, makseinstrumendi või turvaelementide kohta käiv teave ei kattu täielikult ei kliendiandmete, makse saaja ja maksekonto andmete ega ka üksnes maksetehingu andmetega. Kliendi või konto tuvastamine ei näita veel, kuidas tehing tehniliselt tehti või milliseid autentimisvahendeid kasutati. Just seadme, makseinstrumendi või turvaelementide kohta käiv info võib osutada, et näiliselt erinevad tehingud on tegelikult omavahel seotud, näiteks kui need on tehtud sama seadme või sama maksevahendi abil. Selline teave võib olla määrava tähtsusega, et eristada kliendi tavapärast maksekäitumist olukorrast, kus maksevahendit või autentimisvahendeid on väärkasutatud.

Andmeteks on näiteks seadme- ja sessiooniandmed ning muud pettuse tuvastamist võimaldavad tehnilised andmed, mille alusel saab tuvastada, kas makse algatamise keskkond on ebatavaline, näiteks seadme-ID, brauser, IP-aadress. See aitab tuvastada, kas erinevate isikute kontodelt algatatakse makseid sama seadmega või samalt IP-aadressilt, kuigi isikud on erinevates piirkondades. Nende andmete jagamine aitab makseteenuse pakkujatel tuvastada pettuse toimepanemist laiemalt erinevate makseteenuse pakkujate üleselt, mida üks neist oma andmete pinnalt ei pruugi tuvastada. Samuti aitab teabe edastamine PPA-le siduda üksikjuhtumeid laiemate petuskeemidega. Seega aitab andmete avaldamise õigus otseselt kaasa eelnõu eesmärgi saavutamisele. Osaliselt on tegemist tehniliste andmetega, mille privaatsusriive on väiksem, kui näiteks maksetehingu kohta avaldatavate andmete puhul, kuid samas võib tekkida oht, et selliste andmete laialdane jagamine koos muu infoga võib võimaldada isiku tegevuse kohta laiemalt teada saada. Seepärast on lubatud on üksnes niisuguste tehniliste tunnuste jagamine, mis on pettusmustri tuvastamiseks vajalikud, mitte kogu tehnilise logi või autentimisajaloo avaldamine.

5. Andmed maksetehinguga seotud pettuse või muu süüteo tunnustele vastava teo kohta

Need on nn pettuseindikaatorid, mis kirjeldavad petuskeemi toimimist, nagu näiteks tehingu ajastus ja korduvad summad ning mitme isiku samasugused käitumisjooned. See aitab pettuste

toimepanemist avastada näiteks olukorras, kus mitmed kliendid saavad samal päeval panga nimel petukõnesid, siis on võimalik jagada pettusekatsete mustreid teiste krediidiasutustega ning tuvastada nn saripettuse toimepanemine võimalikult vara ka teistel krediidiasutustel ning seeläbi kahjusid vähendada. Sellise teabe avaldamine on eesmärgi saavutamiseks sobiv, sest üksnes kliendi, konto või tehingu tehnilistest andmetest ei pruugi piisata, et tuvastada saripettuse mustrit või erinevate makseteenuse pakkujate juures ilmnenud juhtumite seost. Näiteks olukord, kus mitmed kliendid saavad samal päeval krediidiasutuse nimel petukõnesid, siis on võimalik jagada pettusekatsete mustreid teiste krediidiasutustega ning tuvastada nn saripettuse toimepanemine võimalikult vara ka teistel krediidiasutustel ning seeläbi kahjusid vähendada. Vähem riivavam lahendus oleks näiteks üksnes neutraalse tehnilise info jagamine, kuid see ei oleks eesmärgi saavutamiseks sobiv, sest ei võimaldaks tuvastada konkreetset võimalikku maksetehinguga seotud pettust ning eristada seda lihtsalt maksetehingust, mis on tvapärasega võrreldes ebatavaline. Selliseid andmeid tohib avaldada ainult konkreetse juhtumi puhul ning mitte üldise riskiprofiili loomiseks.

6. Andmed pettuse teel tehtud tehingute või pettusekatsete ja nende asjaolude kohta

Kõnealune meede on eesmärgi saavutamiseks sobiv. Pettuse teel tehtud tehingute või pettusekatsete ja nende asjaolude kohta käiv teave võimaldab makseteenuse pakkujatel tuvastada korduvaid pettusmustreid, seostada omavahel üksikjuhtumeid ning tuvastada kiiremini olukordi, kus sama skeemi kasutatakse mitme makseteenuse kasutaja või mitme makseteenuse pakkuja suhtes. Need andmed võimaldavad edasi anda pettuste mustrit, ehk selline info aitab ära tunda saripettusi ja katkestada sama skeemi edasise kasutamise. Nimetatud andmete avaldamine aitab kaasa seaduse eesmärgi saavutamisele.

Meede on ka vajalik, sest sama eesmärki ei ole võimalik saavutada üksnes anonümiseeritud või statistilise info edastamisega, sest siis ei oleks võimalik tuvastada, et eri juhtumid kuuluvad tegelikult sama petuskeemi alla. Pettusekatsete ja nende asjaolude kirjeldus võimaldab mõista ja ära tunda, milles sarnasus teiste juhtumitega seisneb. Vähem riivav abinõu oleks näiteks ainult üldiste hoiatusmustrite jagamine ilma konkreetsete juhtumite asjaoludeta, kuid see ei oleks sama tõhus, sest ei võimaldaks konkreetseid juhtumeid omavahel seostada.

Meetme mõõdukuse puhul tuleb kaaluda ühelt poolt riive intensiivsust ja teiselt poolt selle abil saavutatava hüve kaalukust. Selliste andemete avaldamine võib anda infot selle kohta, kas konkreetse isik või konto võib olla seotud pettusega ning seetõttu käsitada neid nn kõrgendatud riskiga. Kui pettusekahtlus hiljem ei kinnitu ei tohi see isikut negatiivselt mõjutada. Sellise info avaldamine võib mõjutada asjaomase isiku või konto käsitamist kõrgendatud riskiga objektina ning seetõttu puudutab see lisaks privaatsusele ka mainehuve. Eriti tundlik on see olukorras, kus pettusekahtlus hiljem ei kinnitu. Seetõttu ei tohi seda andmekategooriat tõlgendada kui alust süü omistamiseks või lõpliku õigusliku hinnangu andmiseks. Avaldama peaks faktilised asjaolud ja mustrid, mis on objektiivselt põhjendatud ning see iseenesest ei tohi olla järelduseks, et tehing on tehtud pettuse teel või isik on seotud pettusega.

Teisalt just pettusekatsete ja pettuse teel tehtud tehingute asjaolude jagamine võimaldab kõige tõhusamalt avastada saripettusi, kaitsta teisi võimalikke kannatanuid, takistada sama skeemi korduvat kasutamist ning piirata tekkiva kahju ulatust. Kui sellist teavet ei saaks jagada, väheneks oluliselt makseteenuse pakkujate ja PPA võimekus avastada saripettusi, mis

joonistuvad välja mitmete juhtumite võrdlemisel. See aitab kaitsta isikute vara, maksesüsteemi usaldusväärsust ning aitab pettusi avastada ja välja selgitada. Andmeid tohiks avaldada üksnes siis, kui on objektiivne kahtlus konkreetse tehingu osas, mitte laiemalt üldise riskihinnangu põhjal. Sellise teabe avaldamine iseenesest ei tohi muutuda isiku üldiseks riskiprofiiliks, mis võib mõjutada isikut väljaspool seda konkreetset juhtumit. Arvestades eeltoodut saab pidada nimetatud andmete avaldamist proportsionaalseks ega moonuta põhiõiguste olemust. Andmete avaldamise hüve on kaalukas, sest aitab suures ulatuses avastada erinevaid petuskeeme ja mustreid makseteenuse pakkujate üleselt ning samuti suureneb PPA võimekus pettusi avastada. RIA täidab küberturvalisuse seaduse tähenduses küberintsidentide käsitlemise üksuse ülesandeid ning koordineerib küberintsidentide käsitlemist ning kõnealused andmed aitavad RIA-l tuvastada, ennetada ja ohjata maksepettustega seotud küberintsidente ning pettusmustreid. Need andmed aitavad mõista, milline tehniline või käitumuslik muster viitab pettusele, mis võib osutada laiemale küberohule.

4.2 Maksejuhise kättesaamise edasilükkamise põhiseaduspärasus

Kavandatav VÕS § 724^7 annab maksja makseteenuse pakkujale õiguse objektiivselt põhjendatud pettusekahtluse korral maksejuhise kättesaamine ajutiselt edasi lükata, rakendada lisaturvameetmeid ning vajaduse korral keelduda maksejuhise täitmisest. Regulatsioon riivab eeskätt maksja omandipõhiõigust, täpsemalt PS § 32 lõikes 2 tagatud õigust oma vara vabalt kasutada ja käsutada, kuna rahaliste vahendite kasutamist võib ajutiselt edasi lükata.

Meede on eesmärgi saavutamiseks sobiv. Kui makseteenuse pakkujal tekib objektiivselt põhjendatud kahtlus, et maksejuhis ei ole maksja poolt autoriseeritud või on autoriseeritud pettuse, andmete väärkasutamise või maksja manipuleerimise teel, võimaldab maksejuhise kättesaamise ajutine edasilükkamine ja täiendavate turvameetmete rakendamine kontrollida, kas maksejuhis vastab maksja tegelikule tahtele.

Meede on vajalik. Vähem koormavad meetmed ei võimaldaks sama tõhusalt saavutada eesmärki tõkestada pettuse teel tehtud maksetehinguid. Kliendi tugev autentimine ei ole kõikide pettuse liikide puhul alati piisav, sest isiku manipuleerimise teel kinnitab ta maksejuhise ise. Uued pettuseliigid põhinevad üha enam maksja manipuleerimisel, mis nõuab lisameetmeid lisaks tavapärasele autentimisele. Petturid kannavad rahalised vahendid kiiresti edasi teistele kontodele ja välisriiki ning raha tagasisaamine on raske kui mitte võimatu. Seetõttu ei ole sama eesmärgi saavutamiseks olemas leebemat meedet, mis võimaldaks enne maksejuhise täitmist tõkestada pettuse toimepanemist.

Meede on ka mõõdukas ehk proportsionaalne kitsamas tähenduses. Maksejuhise kättesaamise edasilükkamine on lubatud juhul, kui on objektiivselt põhjendatud kahtlus, et tegemist võib olla pettusega. Samuti nähakse ette, et makseteenuse pakkuja ei saa tugineda üksnes makse saaja kontrollimise teenusele või pelgalt sellele, et maksejuhis tundub ebatavaline või arusaamatu. Lisaks on maksejuhise kättesaamise edasilükkamine ajutine ning ajaliselt piiratud, see on lubatud üksnes seni kuni täiendav kontroll on lõpetatud ning lähtuma peab eelkõige kehtivast VÕS-i regulatsioonist, et maksja makseteenuse pakkuja peab tagama, et maksesumma laekuks saaja makseteenuse pakkuja kontole hiljemalt maksejuhise kättesaamisele järgneval

arvelduspäeval. Meede riivab küll makseteenuse kasutaja õigust oma rahalisi vahendeid kasutada, kuid samas on selle eesmärk kaitsta isiku rahalisi vahendeid.

5. Eelnõu terminoloogia

Eelnõus ei kasutata uusi termineid.

6. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu on vastavus järgmiste Euroopa Liidu õigusaktidega:

- Euroopa Parlamendi ja nõukogu direktiiviga (EL) 2015/2366 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 (ELT L 337, 23.12.2015, lk 35–127) ning
- Parlamendi ja nõukogu määrusega (EL) 2024/886, millega muudetakse määrusi (EL) nr 260/2012 ja (EL) 2021/1230 ning direktiive 98/26/EÜ ja (EL) 2015/2366 eurodes välkkreeditkorralduste osas (ELT L, 19.3.2024.).

7. Seaduse mõjud

Seaduse rakendamise peamine mõju on seotud finantspettuste ennetamise ja tõkestamisega ning maksete turvalisuse suurendamisega. Muudatused mõjutavad eelkõige majandust, riigiasutuste töökorraldust ja sotsiaalvaldkonda ning puudutavad peamiselt makseteenuse pakkujaid (krediidiasutusi ja makseasutusi ja e-raha asutusi), makseteenuse kasutajaid ning pettuste tõkestamisega tegelevaid riigiasutusi.

Majanduslik mõju avaldub peamiselt krediidiasutustele, kellel tekib selgem õiguslik alus pettusekahtlusega maksete peatamiseks ja pettustega seotud teabe jagamiseks, mis aitab vähendada pettustest tulenevat kahju ja suurendab maksesüsteemi usaldusväärsust. Sotsiaalne mõju seisneb maksete suuremas turvalisuses ja elanike finantsilise turvatunde paranemises. Riigiasutuste (PPA ja RIA) töökorraldust mõjutab eelkõige parem teabevahetus.

Muudatused ei avalda mõju elu- ja looduskeskkonnale, riigi julgeolekule ja välissuhetele ega regionaalarengule. Kokkuvõttes on muudatustega kaasnev mõju valdavalt positiivne ning kaasnev ebasoovitavate mõjude risk on madal.

7.1 Nähakse makseteenuse pakkujatele ette õigus keelduda maksejuhiste täitmisest

Sihtrühm nr 1: mõju makseteenuse pakkujatele

Muudatus avaldab mõju kõikidele Eestis tegutsevatele krediidiasutustele ning makseasutustele ja e-raha asutustele.

Mõju ulatus: Mõju ulatust saab pidada väikeseks, kuna täpsustatakse maksejuhise täitmisest keeldumise alust, kuid see ei muuda makseteenuse pakkujate igapäevast maksete täitmise praktikat. Makseteenuse pakkujad kontrollivad ka praegu, kas makse on autoriseeritud ning

korrektselt autenditud. Mõju ulatust on keeruline täpselt hinnata, kuid pigem on see väike, kuna kõnealune õigus puudutab väikest osa kõikidest maksetehingutest, valdav enamus makseid on autoriseeritud ning korrektselt autenditud. Maksejuhise täitmisest keeldumised kõnealusel põhjusel on harvad võrreldes maksetehingute koguarvuga.

Mõju avaldumise sagedus: Mõju avaldamise sagedust on keeruline hinnata, sest ei ole võimalik täpselt välja tuua, et kui palju sellist lisaturvameetmete rakendamise õigust kasutatakse. Võib eeldada, et avaldumise sagedus võrreldes maksete koguarvuga on pigem väike. Lisaturvameetmeid on õigus rakendada ette nähtud kriteeriumite alusel, mitte umbmääraste põhjenduste alusel laiemalt. Ka praegu teostavad makseteenuse pakkujad maksejuhiste puhul turvakontrolle ning tegemist ei ole nn uue režiimi loomisega.

Ebasoovitavate mõjude avaldumise risk: Selline mõjude avaldumise risk on väike. Tegemist on positiivset mõju omava muudatusega, sest makseteenuse pakkujad saavad selge õigusliku aluse rakendada lisaturvameetmeid ning vajadusel maksejuhise täitmisest keeldumiseks, mis aitab pettuste tõkestamise eesmärki saavutada.

Sihtrühm 2. mõju makseteenuse kasutajatele

Muudatus avaldab potentsiaalselt mõju kõikidele makseteenuse kasutajatele, kes igapäevaselt makseid teevad. Ka siinkohal on keeruline hinnata, kui suurele osale makseteenuse kasutajatest see tegelikult mõju avaldab, kuna ei ole üheselt prognoositav, kui palju makseteenuse pakkujad maksete täitmisel sellist õigust kasutavad. Enamus makseid on siiski korrektselt autenditud ning isiku enda pool autoriseeritud.

Mõju ulatus: Mõju ulatust saab pidada pigem väikeseks, kuna isikud puutuvad igapäevaselt sellega kokku harva ja üksikjuhtumitel sest lisaturvakontrolli ei kasutata kõikide maksete puhul. Enamik maksetehinguid täidetakse tavapäraselt ning maksejuhised vastavad üldjuhul makseteenuse lepingus sätestatud tingimustele ning tugev autentimine on tehniliselt nõuetekohane ja maksejuhis on isiku poolt autoriseeritud.

Mõju avaldumise sagedus: Mõju avaldumise sagedus on väike, kuna eelnõu ei näe ette, et kõikide maksete puhul tuleb lisaturvameetmeid rakendada ning maksejuhise kontrolle teostatakse kõikide maksete puhul ka praegu. Lisaturvameetmete rakendamisega puutuvad isikud kokku ebaregulaarselt ja üksikute maksete korral, kui on täidetud selle rakendamise tingimused. Seetõttu võib eeldada, et makseteenuse kasutajad ei puutu pärast muudatust sagedasti kokku lisaturvameetmete rakendamisega ning maksejuhise täitmisest keeldumisega.

Ebasoovitavate mõjude avaldumise risk: Sellise mõju avaldumise risk on madal, tegemist on positiivset mõju omava muudatusega, sest aitab kaasa pettuste tõkestamisele. Muudatus aitab ennetada pettusi ning vähendada isikutele rahalise kahju tekkimise riski. Kuigi üksikjuhtudel võib isiku makse täitmine pettusekahtluse tõttu ajutiselt viibida, on selle eesmärk makseteenuse kasutaja kaitse ning maksete turvalisuse suurendamine.

7.2 Nähakse makseteenuse pakkujatele ette õigus avaldada pettuste avastamise ja väljaselgitamise eesmärgil andmeid ja teavet

Sihtrühm 1. Makseteenuse pakkujad

Muudatus võib mõju avaldada kõikidele Eestis tegutsevatele makseteenuse pakkujatele.

Mõju ulatus: Makseteenuse pakkujate jaoks on muudatuse mõju pigem keskmine, kuna andmete avaldamine on ette nähtud õigusena, mitte kohustusena ning seda võib teha juhul, kui makseteenuse pakkujal on objektiivselt põhjendatud kahtlus, et klient või maksetehing võib olla seotud pettusega. Pettuste avastamine ja väljaselgitamine on makseteenuse pakkujate igapäevane tegevus ning sellel eesmärgil ka juba vajalikke andmeid töödeldakse. Muudatus aitab paremini pettusi avastada ja välja selgitada ning koostöö teiste makseteenuse pakkujatega ning PPA-ga aitab vähendada pettustega tekitatud kahju, mistõttu on tegemist positiivse mõjuga.

Mõju avaldumise sagedus: Mõju avaldumise sagedust on keeruline hinnata, kuid arvestades maksete koguarvuga saab seda pidada pigem väikeseks, sest andmete avaldamine on lubatud ette nähtud tingimustel ning mitte laialdaselt kõikide maksetehingute puhul. Arvestades, et enamus makseid on korrektselt autenditud ja autoriseeritud, on andmete avaldamine pigem erandlik.

Ebasoovitavate mõjude avaldumise risk: Selline risk on madal, tegemist on positiivse muudatusega, mis aitab makseteenuse pakkujatel efektiivsemalt pettusi tõkestada. Arvestades, et andmete avaldamine on lubatud kindlal eesmärgil ning on ette nähtud õigusena, mitte kohustusena, ei ole põhjust eeldada negatiivset mõju makseteenuse pakkujate tavapärasele tegevusele.

Sihtrühm 2. Makseteenuse kasutajad

Muudatus avaldab potentsiaalselt mõju kõikidele makseteenuse kasutajatele, kuid igapäevaselt siiski väikesele osale makseteenuse kasutajatest, sest pettuste osakaal kogu maksetehingute arvust on väike.

Mõju ulatus: Makseteenuse kasutajate jaoks on muudatuse mõju kaudne. Muudatus ei mõjuta makseteenuste kasutamist üldiselt, vaid puudutab üksnes neid olukordi, kus esineb põhjendatud pettuse kahtlus ning makseteenuse pakkuja avaldab pettuse avastamise ja väljaselgitamise eesmärgil isiku andmeid.

Mõju avaldumise sagedus: Mõju avaldumise sagedus on pigem väike, sest muudatus ei mõjuta makseteenuse kasutajat igapäevaselt ning kokkupuude sellega on ebaregulaarne ja harv. Eelnõu näeb andmete avaldamiseks ette kriteeriumid ning makseteenuse pakkujatel ei ole õigust jagada andmeid laiemalt ebamäärastel eesmärkidel. Mõju avaldub üksnes olukordades, kus andemete avaldamine on vajalik pettuse avastamise ja väljaselgitamise eesmärgil.

Ebasoovitavate mõjude avaldumise risk: Selline risk on pigem madal, tegemist on positiivset mõju omava muudatusega. See aitab vähendada rahalise kahju tekkimise riski ning suurendab maksete turvalisust. Andmeid tohib avalda üksnes piiratud ulatuses ja eesmärgil. Samas võib avalduda risk, et andmeid isiku kohta avaldatakse pettusekahtluse korral, kus see kahtlus kinnitust ei leia, ehk et tegemist on valepositiivse kahtlusega. Samas ei ole selliste juhtumite täielik välistamine võimalik ning andmete avaldamise eesmärgiks on isiku kaitsmine pettuse ohvriks langemise eest. Nimetatud juhul ei tohi andmete avaldamine isikule kaasa tuua mingeid negatiivsed tagajärgi. Makseteenuse pakkujad peavad siinkohal rangelt kinni pidama andmete minimaalsuse ja eesmärgipärase töötlemise põhimõtetest. Andmete avaldamine peab olema logitud ning tagantjärele kontrollitav. Isikul peab olema õigus teada saada, milliseid tema andmeid ja kellele edastati. Seda ulatuses, millises on makseteenuse pakkujal seaduse järgi õigus avaldada, arvestades muuhulgas näiteks rahapesu ja terrorismi rahastamise tõkestamise seadusest tulenevaid piiranguid.

Sihtrühm 3. Politsei- ja Piirivalveamet

Muudatus avaldab mõju PPA-le.

Mõju ulatus: PPA-le tähendab muudatus laiemat ligipääsu pettustega seotud andmetele, mis parandab oluliselt petuskeemide tuvastamist ning seostamist ja parandab selles osas PPA võimekust. Seeläbi paraneb PPA ennetav töö. Muudatus ei too kaasa PPA-le täiesti uue ülesande tekkimist ega muudatusi töökorralduses.

Mõju avaldumise sagedus: PPA jaoks ei saa pidada mõju avaldumise sagedust suureks. PPA tegeleb ka praegu igapäevaselt pettuste tõkestamisega ning andmete edastamine parandab sellist võimekust. Mõju sagedus on üksikjuhtumi põhine, kui makseteenuse pakkuja avaldab pangasaladust konkreetse pettuse kahtluse korral.

Ebasoovitavate mõjude avaldumise risk: Selline risk on väike, tegemist on positiivset mõju omava muudatustega, mis aitab parandada pettuste tõkestamise võimekust.

Sihtrühm 4. Riigi Infosüsteemi Amet

Mõju ulatus: Muudatus annab RIA-le võimaluse saada makseteenuse pakkujalt piiratud ulatuses teavet maksetehingutega seotud pettuste ja pettusekatsete asjaolude ning kasutatud tehniliste vahendite kohta.

Mõju RIA tegevusele seisneb selles, et täieneb sisend küberintsidentide analüüsiks ja riskihindamiseks ning seeläbi suureneb võimekus info töötlemiseks ja seostamiseks olemasoleva küberohuteabega. RIA pädevus ei muutu – amet täidab ka kehtiva õiguse alusel küberintsidentide käsitlemise, riskide seire ja ohtudest teavitamise ülesandeid.

Mõju avaldumise sagedus: Mõju avaldub juhtumipõhiselt, sõltuvalt maksetehingutega seotud pettuste ja pettusekatsete arvust ning makseteenuse pakkuja hinnangust objektiivselt põhjendatud kahtluse olemasolule. Arvestades, et maksepettused on sagedased ning sageli

seotud infosüsteemide ründamise või autentimisvahendite kuritarvitamisega, võib RIA-le edastatava info hulk olla regulaarne, kuid tegemist ei ole automaatse ega pideva andmevooga.

Ebasoovitavate mõjude avaldumise risk: Sellist riski saab hinnata väikeseks - RIA-le avaldatav andmekoosseis on kitsalt piiritletud ega hõlma otseseid kliendi tuvastus- ega kontoteavet. Krediidiasutused edastavad andmeid juhtumipõhiselt ning selliste andmete töötlemine eeldatavalt RIA töökoormust ei suurenda.

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

Seaduse rakendamisega ei kaasne tulusid ega kulusid riigieelarvele ning eelnõu ei ole seotud kohalike omavalitsuste tegevusega.

PPA-l ja RIA-l on vaja teha tehnilisi ja korralduslikke ettevalmistusi turvaliseks ja sihipäraseks andmevahetuseks krediidiasutustega. Tegemist on nende asutusete jaoks olemasolevate tööprotsesside täpsustamisega ning see ei eelda täiendavaid kulusid.

9. Rakendusaktid

Käesoleva seadusega ei kehtestata uusi rakendusakte ega muudeta olemasolevaid. Samuti ei kaasne seadusega rakendusaktide kehtetuks muutumist.

10. Seaduse jõustumine

Seadus jõustub üldises korras.

11. Eelnõu kooskõlastamine ja huvirühmade kaasamine

Eelnõu esitati kooskõlastamiseks ja arvamuse avaldamiseks Justiits- ja Digiministeeriumile, Siseministeeriumile, Politsei- ja Piirivalveametile, Eesti Pangale, Eesti Pangaliidule, Riigi Infosüsteemi Ametile, Finantsinspektsioonile, Eesti Infotehnoloogia ja Telekommunikatsiooni Liidule.

Eelnõule esitasid arvamuse Justiits- ja Digiministeerium, Siseministeerium, Eesti Pank, Eesti Pangaliit, Riigi Infosüsteemi Amet ning Finantsinspektsioon. Esimese kooskõlastusringil esitatud märkused ning Rahandusministeeriumi selgitused on leitavad seletuskirjale lisatud kooskõlastustabelist.

Lähtuvalt esitatud märkustest on eelnõu muudetud ning arvestades esitatut on eelnõu paragrahvide sõnastus ning eelnõu struktuur oluliselt muutunud. Muudatused on tehtud eelkõige eelnõu paragrahvis 1. Vaatamata paragrahvide sõnastuste muutmisest ning uutest lisatud lõigetest ei ole eelnõu sisu muutunud.

Algatab Vabariigi Valitsus ….. 2026. a

Vabariigi Valitsuse nimel

(allkirjastatud digitaalselt)
Heili Tõnisson
Valitsuse nõunik