Võlaõigusseaduse ja krediidiasutuste seaduse muutmise seaduse eelnõu (finantspettuste ennetamine ja tõkestamine) 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 annab krediidiasutustele selge õigusliku aluse pettusekahtlusega seotud info vahetamiseks teiste krediidiasutuste ning Politsei- ja Piirivalveametiga (edaspidi *PPA*) ja Riigi Infosüsteemi Ameti (edaspidi *RIA*) küberintsidentide käsitlemise osakonna CERT-EE-ga (edaspidi *CERT*). Samuti loob eelnõu selgema õigusraamistiku ja tugevdab pankade õigust põhjendatud pettuse kahtluse korral makseid ajutiselt peatada või makse täitmisest keelduda.

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.

Teiseks, eelnõuga muudetakse krediidiasutuste seadust (edaspidi *KAS*), millega antakse krediidiasutustele õigus jagada vajalikku teavet pettuste avastamiseks, väljaselgitamiseks ja ennetamiseks. Seda juhul kui krediidiasutusel on objektiivselt põhjendatud alus kahtlustada, 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, Politsei- ja Piirivalveametiga (edaspidi *PPA*) ning Riigi Infosüsteemi Ametiga (edaspidi *RIA*).** Kehtivas õiguses selline õigus puudub ning see on osutunud probleemiks pettuste avastamisel ja tõkestamisel. 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.

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

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, 11.11.2025, 10;
- Võlaõigusseadust redaktsioonis RT I, 11.11.2025, 16.

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. Selle 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]

Seaduseelnõule ei ole koostatud väljatöötamiskavatsust ega ka õiguslikke valikuid kajastavat kontseptsiooni, sest eelnõu on kiireloomuline. Seadus on plaanitud jõustuma 2026. aasta 1. juulil.

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 ennetamist 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.

[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

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.

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

Käesolev eelnõu lähtub samast eesmärgist ning loob riigisiseses õiguses vajalikud õiguslikud alused, mis aitavad pettusi tõhusamalt ennetada ja tõkestada. Eesmärk on võimaldada selliste meetmete rakendamist teatud ulatuses juba enne, kui hakkab kehtima uus makseteenuste määrus. Arvestades pettuste jätkuvat kasvu ning nende suur 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.

3. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb kolmest paragrahvist, millest viimases nähakse ette seaduse jõustumine.

Eelnõu §-ga 1 muudetakse VÕS-i.

Eelnõu § 1 punktiga 1 täiendatakse VÕS § 724^3 lõigetega 4^1–4^3 ning nähakse ette, et makseteenuse pakkuja võib keelduda autoriseeritud maksejuhise täitmisest, kui pärast komisjoni delegeeritud määruses (EL) 2018/389[9] (edaspidi *komisjoni delegeeritud määrus*) ette nähtud turvameetmete täiendavat rakendamist on makseteenuse pakkujal põhjendatud kahtlus, et maksetehingu täitmiseks antud nõusolek on saadud andmete väärkasutamise, pettuse või maksja manipuleerimise teel.

Makseteenuse pakkujad peavad kasutama autentimisel turvalist teabevahetamise viisi ning rakendama turvameetmeid, mis tagavad isikustatud turvaelementide konfidentsiaalsuse ja andmete tervikluse. Komisjoni delegeeritud määruse artikli 2 lõike 1 kohaselt peavad makseteenuse pakkujatel turvameetmete rakendamise eesmärgil olema tehinguseiremehhanismid, mis võimaldavad neil avastada autoriseerimata või pettuse teel tehtud maksetehinguid. Need

[5] maksete-ulevaade-2025_2-avalik.xlsx
[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
[9] Delegated regulation - 2018/389 - EN - EUR-Lex

mehhanismid peavad tuginema maksetehingute analüüsile, mille juures võetakse arvesse elemente, mis on makseteenuse kasutajale iseloomulikud isikustatud turvavolituste tavapärase kasutamise puhul.

Komisjoni delegeeritud määruse 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.

Komisjoni delegeeritud määruse artikkel 18 käsitleb tehingu riskianalüüsi ning puudutab olukorda, kus makseteenuse pakkujatele antakse luba mitte kasutada kliendi tugevat autentimist juhul, kui maksja algatab elektroonilise kaugmaksetehingu, mille makseteenuse pakkuja on tehinguseiremehhanismide alusel lugenud väikese riskiga tehinguks. Seda, kas tegemist on väikese riskiga tehinguga, tuleb hinnata reaalajas toimuva riskianalüüsi käigus. Hinnata tuleb näiteks järgmisi asjaolusid:

- 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.

Kehtiv VÕS ei näe aga otseselt ette, et juhul, kui selles komisjoni delegeeritud määruses nimetatud turvameetmete rakendamisel tekib makseteenuse pakkujal põhjendatud kahtlus, et maksetehingu täitmiseks antud nõusolek on saadud andmete väärkasutamise, pettuse või maksja manipuleerimise teel, on tal õigus autoriseeritud maksejuhise täitmisest keelduda.

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 delegeeritud määruses 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 delegeeritud määruses, kui 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.

VÕS § 724^3 uus lõige 4^2 – see sätestab, et kui sama paragrahvi lõikes 4^1 nimetatud turvameetmete täiendava rakendamise tulemusel makse täidetakse hilinemisega, kohaldatakse VÕS § 733^3

lõigetes 4^1 ja 4^2 makse hilinenud täitmise kohta sätestatut. VÕS § 733^3 lõiked 4^1 ja 4^2 käsitlevad väärtuspäeva korrigeerimist hilinenud makse korral. Eelnõuga VÕS-i lisatav § 724^3 lõige 4^1 näeb ette õiguse turvameetmete täiendavaks rakendamiseks. See tähendab, et juhul, kui makseteenuse pakkuja on teinud tehingu riskianalüüsi ning tekib kahtlus, et maksetehingu täitmiseks antud nõusolek on saadud andmete väärkasutamise, pettuse või maksja manipuleerimise teel, on õigus rakendada täiendavaid turvameetmeid. 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 makse saaja olukord, kuna kontole laekunud raha väärtuspäevaks loetakse algselt makse nõuetekohaseks täitmiseks ette nähtud kuupäev, isegi kui raha jõuab vastavale kontole tegelikult hiljem.

VÕS § 724^3 uus lõige 4^3 – selle kohaselt tuleb välkkreeditkorralduse puhul maksejuhise täitmisest keelduda kooskõlas välkmaksete määrusega. Välkmaksete määruse kohaselt teeb makse saaja makseteenuse pakkuja kümne sekundi jooksul alates maksja makseteenuse pakkujalt välkkreeditkorralduse maksekäsundi vastuvõtmise ajast maksetehingu summa makse saaja maksekontol kättesaadavaks vääringus, milles makse saaja konto on nomineeritud, ning kinnitab maksja makseteenuse pakkujale maksetehingu lõpuleviimist. See tähendab, et makseteenuse pakkuja peab maksetehingu riskianalüüsi ära tegema kümne sekundi jooksul ning otsustama, kas on vajalik turvameetmete täiendav rakendamine. **Juhul, kui maksetehingu riskianalüüsi põhjal selgub, et vajalik on turvameetmete täiendav, siis täidetakse maksejuhis pärast täiendavat kontrolli ning sellisel juhul ei rakendu välkmaksete määruse kümne sekundi nõue. Turvameetmete täiendav rakendamine peab toimuma aga ilma ebamõistliku viivituseta.**

Eelnõu § 1 punktiga 2 muudetakse VÕS § 724^6 lõiget 2 ning asendatakse läbi EL direktiivi 2015/2366/EL artikli 98 tehtud viide Euroopa Komisjoni rakendusmäärusele konkreetse rakendusmäärusega, milleks on Komisjoni delegeeritud määrus (EL) 2018/389. Kuna esimest korda on delegeeritud määrusele viidatud VÕS § 724^3 lõikes 4^1, siis siin kasutatakse lühivormi.

Eelnõu § 1 punktiga 3 täiendatakse VÕS § 733^9 lõikega 3 ning nähakse ette, et makseteenuse pakkuja ei vastuta kahju eest, kui käesoleva seaduse § 724^3 lõike 4^1 alusel ette nähtud turvameetmete täiendava rakendamise tulemusel täidetakse makse hilinemisega, tingimusel, et nimetatud turvameetmete rakendamine viiakse läbi põhjendamatu viivituseta ning rakendamise aluseks on objektiivselt põhjendatud kahtlus, et maksetehingu täitmiseks antud nõusolek on saadud andmete väärkasutamise, pettuse või maksja manipuleerimise teel. Kui makseteenuse pakkuja rakendab maksetehingu kontrollimiseks täiendavaid turvameetmeid võib selle peale kuluda rohkem aega, kui on ette nähtud maksetehingu täitmiseks. Alati ei pruugi turvameetmete täiendava 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.

Eelnõu §-ga 2 muudetakse krediidiasutuste seadust, **mille kohaselt täiendatakse KAS-i uue §-ga 89^4.**

Nagu eespool juba märgitud, siis uus paragrahv annab krediidiasutustele selged õiguslikud alused jagada vajalikku teavet pettuste avastamiseks, väljaselgitamiseks ja ennetamiseks juhul, kui

krediidiasutusel on objektiivselt põhjendatud alus kahtlustada, et klient või maksetehing võib olla seotud pettusega. Kehtiv KAS § 88 reguleerib iseenesest juba pangasalduse 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 kui 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 kustutada kui tulevikus hakkab kehtima eespool nimetatud EL makseteenuste määrus (ehk ka õigustehniliselt on lihtsam kustuda eraldiseisvat §-i).

KAS uue §-i 89^4 lõike 1 kohaselt antakse krediidiasutusele õigus avaldada erinevat teavet, mh pangasaladust teisele krediidiasutusele ning Politsei- ja Piirivalveametile maksetehingutega seotud pettuste avastamiseks, väljaselgitamiseks ja ennetamiseks juhul, kui krediidiasutusel on objektiivselt põhjendatud alus kahtlustada, et klient või maksetehing võib olla seotud pettusega. Pettuste tõkestamisel on oluline kiirus ning koostöö, et oleks võimalik operatiivselt sekkuda. Kehtiv KAS § 88 lg 5 p 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 ennetamist olukordades, kus menetluse alustamine võib toimuda alles pärast esmast juhtumi analüüsi ning pettuse ennetamise ja 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 alus kahtlustada pettust, 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 tuvastamiseks 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 nime ja maksekonto tunnuste 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.

Punktiga 4 nähakse ette andmete ja teave jagamine pettuse teel tehtud tehingute või pettusekatsete ja nende 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 ka makseteenuse osutamisel tuvastatud manipulatsioonitehnikaid 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.

Punkti 5 alusel saab edastada andmeid ja teavet maksetehinguga seotud pettuse või muu süüteo tunnustele vastava teo tuvastamiseks, sealhulgas kasutatud seadmete, makseinstrumendi või turvaelementide kohta. Need 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.

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)[10] mõistes küberturvalisuse pädev asutus ja kontaktpunkt.

Nagu eespool juba märgitud, siis uue paragrahvi kohaselt RIA-le avaldatatavad andmed ei pruugi 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 ning maksetehinguga seotud pettuse või muu süüteo tunnustele vastava teo tuvastamist võimaldavaid andmeid, sealhulgas kasutatud seadmete, makseinstrumendi või turvaelementide kohta. RIA-le ei avaldata

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

andmeid ja teavet 1) kliendi tuvastamiseks; 2) makse saaja ja maksekonto kohta ning 3) maksetehingute kohta, sealhulgas tundlikke 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 CERT-il võimalik väljaspool seda sekkuda küberturvalisust ohustavatele olukordadele. Majandus- ja kommunikatsiooniministeeriumi 25. aprilli 2011. aasta määruse nr 28 „Riigi Infosüsteemi Ameti põhimäärus“ § 8 lg 4 p 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 lg 4 p 4 kohaselt korraldab küberturvalisuse amet küberturvalisust ohustavate riskide seiret, analüüsi ja ohtudest teavitamist. KAS-i lisatav uus paragrahv annab võimaluse avaldada pangasaladust ka olukordades, mis on väljaspool riikliku järelevalve menetlust. See annab võimaluse sekkuda küberintsidentide puhul operatiivselt ja ennetavalt. Andmete avaldamise korral üksnes järelevalve menetluse raames jõuab teave CERT-le liiga hilja ning see takistab CERT-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 kliendi tuvastusandmeid, makse saaja ega maksekonto andmeid ega tundlikke 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, sealhulgas kasutatud seadmete, makseinstrumentide või turvaelementide kohta. Seega on andmete avaldamine suunatud eeskätt tehnilise ja mustripõhise analüüsi võimaldamisele, mitte üksikisikute tuvastamisele.

Eelnõu §-ga 3 sätestatakse jõustumine, milleks on 2026. aasta 1. juuli. Jõustumise aja selgitus on toodud seletuskirja 10. osas „Seaduse jõustumine“.

4. Eelnõu terminoloogia

Eelnõus ei kasutata uusi termineid.

5. 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.).

6. Eelnõu vastavus Eesti Vabariigi põhiseadusele

Kavandatavad muudatused riivavad mitmeid Eesti Vabariigi põhiseadusega tagatud põhiõigusi, eeskätt isiku eraelu puutumatust (PS § 26), omandipõhiõigus (PS § 32) ning ettevõtlusvabadust (PS § 31). Samas on muudatuste eesmärk maksepettuste ennetamine ja tõkestamine, isikute vara kaitse ning finantssüsteemi usaldusväärsuse tagamine.

Eraelu puutumatuse riive

Makseteenustega seotud andmed, sealhulgas maksekonto andmed, maksetehingute teave ning makseinstrumentide ja turvaelementidega seotud andmed, kuuluvad isiku eraelu kaitsealasse. KAS-i muudatused võimaldavad selliste andmete avaldamist teistele krediidiasutustele, PPA-le ning RIA-le pettuste avastamise, väljaselgitamise ja ennetamise eesmärgil. Eraelu puutumatuse riive on siiski piiratud, kuna andmete avaldamine on lubatud üksnes objektiivselt põhjendatud pettusekahtluse korral, selgelt määratletud eesmärgil ning piiratud adressaatide ringile. Samuti on seaduses ammendavalt loetletud andmed, mida võib avaldada.

Omandiõiguse riive

Makseteenuse pakkujale antav õigus keelduda autoriseeritud maksejuhise täitmisest mõjutab maksja võimalust oma rahalisi vahendeid vabalt kasutada ning riivab seeläbi omandiõigust. Teisalt aitab selline õigus pettusi avastada ja tõkestada ning seeläbi vältida isikutel läbi pettuste oma rahalisi vahendeid kaotada. Eelnõu kohaselt on maksejuhise täitmisest keeldumine lubatud üksnes juhul, kui pärast täiendavate turvameetmete rakendamist esineb objektiivselt põhjendatud kahtlus, et maksetehingu täitmiseks antud nõusolek on saadud andmete väärkasutamise, pettuse või maksja manipuleerimise teel.

Muudatused näevad ette, et juhul kui täiendavate turvameetmete rakendamise tulemusel täidetakse makse hilinemisega, kohaldatakse makse hilinenud täitmise kohta kehtivaid sätteid ning makseteenuse pakkuja ei vastuta kahju eest, kui turvameetmed on rakendatud põhjendamatu viivituseta ja objektiivselt põhjendatud kahtluse alusel. Selline vastutuse piiramine on vajalik, et võimaldada makseteenuse pakkujatel pettusekahtluse korral kindlamalt tegutseda, ilma et tuleks karta ebaproportsionaalset vastutust olukordades, kus sekkumine on õigustatud ja vajalik.

Ettevõtlusvabaduse riive

Muudatused mõjutavad ka makseteenuse pakkujate ettevõtlusvabadust, kuna seadusega kaasnevad neile nii õigused kui kohustused pettuste tõkestamisel. Samas annavad muudatused makseteenuse pakkujatele selgema õigusliku aluse sekkumiseks ning vähendavad õiguslikku ebakindlust olukordades, kus kahtlus puudutab makse tegemiseks antud nõusoleku tegelikku päritolu.

Eelnõuga välistatakse makseteenuse pakkujate vastutus juhul, kui põhjendatud pettuse kahtluse korral mõistliku aja jooksul rakendatud turvameetmete tõttu täidetakse makse hilinemisega. Teisalt aitab see vähendada kahjude tekkimist nt ettevõtetele, et nende makse ei jõuaks petturite kontodele. Selge regulatsioon toetab seeläbi ettevõtlusvabaduse tegelikku teostamist.

Sobivus

Valitud meetmed on sobivad eesmärgi saavutamiseks.

Makseteenuse pakkujale antav õigus keelduda maksetehingu täitmisest võimaldab peatada pettuse teel tehtavaid maksetehinguid enne isikutele kahju tekkimist.

Krediidiasutustele pangasaladuse avaldamise õiguse andmine võimaldab pettusi kiiremini avastada ja tõkestada. Andmete vahetamise võimalus ja kiirus on kriitilise tähtsusega, sest isikutelt välja petetud raha kantakse kiiresti teistele kontodele ja selle tagasisaamise tõenäosus on väga väike.

Vajalikkus

Valitud meetmed vajalikud, sest kehtiv õigus ei anna makseteenuse pakkujale piisavalt selget alust maksejuhise täitmisest keeldumiseks pettuste puhul. Maksetehingu puhul on pettuslikule tehingule reageerimine ajakriitiline, kuna kahju tekib väga kiiresti. Vähem piiravad meetmed ei ole piisavad, sest pärast maksejuhise täitmist on isikul oma ülekantud raha tagasisaamise võimalus väga väike.

Mõõdukus kitsamas tähenduses

Meetmed on eesmärgi suhtes proportsionaalsed, sest maksejuhise täitmisest keeldumine on lubatud ainult juhul, kui rakendatud on täiendavad turvameetmed, kahtlus on objektiivselt põhjendatud. Ehk et selle rakendamine on piiritletud.

Makseteenuse pakkujate vastutuse välistamine ei ole absoluutne ning see kehtib juhul, kui turvameetmeid rakendatakse põhjendamatu viivituseta ning kahtlus on objektiivselt põhjendatud.

Pangasaladuse avaldamine on lubatud konkreetse ja selgelt määratletud eesmärgil ning piiratud adressaatide ringile ning pangasaladuse avaldamine on lubatud objektiivselt põhjendatud kahtluse olemasolul. Samuti on andmete liikide loetelu ammendav.

7. Seaduse mõjud

7.1 Nähakse krediidiasutustele ette õigus keelduda maksejuhiste täitmisest

Sihtrühm nr 1: mõju makseteenuse pakkujatele

Muudatus võib mõju avaldada enamikele Eestis tegutsevatele (suurematele) krediidiasutustele. Eestis on hetkeseisuga[11] registreeritud 8 krediidiasutust (kes on saanud Finantsinspektsioonilt tegevusloa) ning 6 välisriigi krediidiasutuse filiaali. Eestis pakuvad teadaolevalt põhimakseteenuseid 7 krediidiasutust: AS LHV Pank, AS SEB Pank, AS TBB pank, Coop Pank AS, Luminor Bank AS ja Swedbank AS. Lisaks pakub põhimakseteenuseid üks Eestis tegutsev välisriigi krediidiasutuse filiaal, milleks on AS Citadele banka Eesti filiaal. Seega hetkel ei paku põhimakseteenuseid: AS Inbank, Bigbank AS, Holm Bank AS.

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

[11] https://www.fi.ee/et/pangandus-ja-krediit/krediidiasutused

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 avaldumise sagedust saab pidada väikeseks seetõttu, et maksejuhise täitmisest keeldumine on pigem erandlik ning puudutab väikest osa maksejuhistest.

Ebasoovitavate mõjude avaldumise risk: Selline mõjude avaldumise risk on väike. Tegemist on positiivset mõju omava muudatusega, sest makseteenuse pakkujad saavad selge õigusliku aluse maksejuhise täitmisest keeldumiseks, mis aitab pettuste tõkestamisel.

Sihtrühm 2. mõju makseteenuse kasutajatele

Muudatus avaldab potentsiaalselt mõju kõikidele makseteenuse kasutajatele, kuid igapäevaselt siiski väikesele osale makseteenuse kasutajatest, kuna enamus makseid on autoriseeritud ning korrektselt autenditud.

Mõju ulatus: Mõju ulatust saab pidada väikeseks, kuna see avaldub harva ja üksikjuhtumites. Enamik maksetehinguid täidetakse tavapäraselt ning maksejuhised vastavad üldjuhul makseteenuse lepingus sätestatud tingimustele ning tugev autentimine on tehniliselt nõuetekohane. Seetõttu on mõju ulatus väike.

Mõju avaldumise sagedus: Mõju avaldumise sagedus on väike, kuna eelnõu ei näe makseteenuse kasutajate vaatest ette uut piirangut maksetehingute tegemisel. Eelnõu täpsustab kehtivat õigust. Seetõttu ei puutu makseteenuse kasutajad pärast muudatust oluliselt sagedamine kokku maksejuhise täitmisest keeldumisega.

Ebasoovitavate mõjude avaldumise risk: Sellise mõju avaldumise risk on madal, tegemist on positiivset mõju omava muudatusega, sest aitab kaasa pettuste tõkestamisele.

7.2 Nähakse krediidiasutustele ette õigus avaldada pettuste tõkestamiseks pangasaladust

Sihtrühm 1. Krediidiasutused

Muudatus võib mõju avaldada enamikele Eestis tegutsevatele krediidiasutustele.

Mõju ulatus: Krediidiasutuste jaoks on muudatuse mõju keskmine, kuid mitte koormav. Pangasaladuse avaldamine on ette nähtud krediidiasutuste õigusena, mitte kohustusena. Pettuste tõkestamine on krediidiasutuste igapäevane tegevus. Muudatus aitab paremini pettusi tõkestada ning koostöö teiste krediidiasutuste ning PPA-ga aitab vähendada pettustega tekitatud kahju, mistõttu on tegemist positiivse mõjuga.

Mõju avaldumise sagedus: Mõju avaldumise sagedus on madal võrreldes kõigi maksetehingute kogumahuga, kuna andmete avaldamine on lubatud üksnes erandlikel juhtudel, kui esineb objektiivselt põhjendatud pettusekahtlus. Valdav enamus maksetehinguid ja makseteenuse kasutajaid ei puutu sellega kokku.

Teisalt pettusejuhtumite sees avaldub muudatus sagedamini, kuna pettused on tihti korduvad ja mitut krediidiasutust hõlmavad.

Ebasoovitavate mõjude avaldumise risk: Selline risk on madal, tegemist on positiivse muudatusega, mis aitab krediidiasutustel efektiivsemalt pettuste tõkestamisel.

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 seisneb muudatuse mõju kaudselt. Muudatus ei mõjuta makseteenuste kasutamist üldiselt, vaid üksnes neid olukordi, kus esineb põhjendatud pettuse kahtlus ning krediidiasutus avaldab teistele pangasaladust. Mõju makseteenuse kasutajale on piiratud konkreetse olukorraga, kus on pettuse kahtlus.

Mõju avaldumise sagedus: Mõju avaldumise sagedus on väike, sest ei mõjuta makseteenuse kasutajat igapäevaselt. Mõju avaldub üksnes olukordades, kus on andemete avaldamine vajalik pettuse tõkestamise eesmärgil.

Ebasoovitavate mõjude avaldumise risk: Selline risk on madal, tegemist on positiivset mõju omava muudatusega. See aitab vähendada rahalise kahju tekkimise riski ning suurendab maksete turvalisust.

Sihtrühm 3. Politsei- ja Piirivalveamet

Muudatus avaldab mõju PPA-le.

Mõju ulatus: PPA tähendab muudatus laiemat ligipääsu pettustega seotud andmetele, mis parandab oluliselt petuskeemide tuvastamist ning seostamist. Seeläbi paraneb PPA ennetav töö.

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 krediidiasutus 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 krediidiasutustelt 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 krediidiasutuste 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.

9. Rakendusaktid

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

10. Seaduse jõustumine

Seadus jõustub 2026. aasta 1. juulil.

Jõustumistähtaeg on ette nähtud arvestusega, et krediidiasutustel oleks võimalik valmistada ette ning teha vajadusel tehnilised muudatused, mis on vajalikudud maksejuhise täitmisest keeldumise rakendamiseks ning samuti, et krediidiasutustel ning PPA-l ja RIA-l oleks võimalik arvestada ning teha vajalikud tehnilised ja korralduslikud ettevalmistused andmete turvaliseks ja sihipäraseks vahetamiseks pettuste ennetamise eesmärgil.

11. Eelnõu kooskõlastamine ja huvirühmade kaasamine

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

Algatab Vabariigi Valitsus ….. 2026. a

Vabariigi Valitsuse nimel

(allkirjastatud digitaalselt)
Heili Tõnisson
Valitsuse nõunik