



Lietuvos Respublikos finansų ministerija  
Lietuvos bankas  
FINTECH Lietuva grupė  
Lietuvos bankų asociacija  
Lietuvos prekybos pramonės ir amatų rūmų asociacija  
Lietuvos smulkiojo ir vidutinio verslo taryba  
Lietuvos vartotojų organizacijų aljansas  
Mokėjimo ir elektroninių pinigų įstaigų asociacija  
Vytauto Didžiojo universitetas  
Fintech Hub LT

<https://www.lb.lt/lt/mokejimu-taryba>  
<http://finmin.lrv.lt/lt/veiklos-sritys/finansu-rinku-politika/mokejimu-taryba>

Galimybių studija

2019 04 18  
Vilnius

# Kliento pažinimo (KYC) proceso optimizavimo galimybės Lietuvoje

Mokėjimų tarybos Kliento pažinimo (KYC) proceso optimizavimo galimybių studijos užduoties grupės ataskaita

**Turinys**

Santrauka	3
1. KYC proceso sąvoka	7
2. Esamo KYC proceso problematika ir optimizavimo nauda	8
3. KYC proceso duomenys	9
4. Valstybės registrų duomenų panaudojamumas KYC procese	11
4.1. Galimybės surinkti registrų duomenis vieno langelio principu	11
4.2. Problematika, susijusi su PEP	12
4.3. Problematika, susijusi su JADIS	13
5. KYC proceso optimizavimo alternatyvos, kitų šalių patirtis	14
5.1. KYC proceso optimizavimo alternatyvos	14
5.2. Tarptautinis kontekstas, suderinamumas su kitomis duomenų bazėmis ir (arba) užsienio sprendimais	16
6. Siūlomas optimizuoto KYC proceso modelis	17
7. KYC API sprendimo valdytojas	19
8. Teisinės KYC proceso optimizavimo kliūtys ir rekomendacijos	21
9. KYC proceso, kai klientas nepilnametis, problematika	24
10. KYC procesas BDAR kontekste	25
10.1. KYC API sprendimo valdytojas: duomenų valdytojas ar tvarkytojas?	25
10.2. Sutartys dėl duomenų teikimo	27
10.3. Teisė būti pamirštam	27
Priedai	29

**Santrumpos**

AMLD5 – penktoji Pinigų plovimo ir terorizmo finansavimo prevencijos direktyva (2018 m. gegužės 30 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/843)

API – taikomosios programinės sąsajos (angl. *Application Programming Interface*), skirtos integracijai su kitomis informacinėmis sistemomis kurti

BDAR – Bendrasis duomenų apsaugos reglamentas

EK – Europos Komisija

ES – Europos Sąjunga

FĮ – finansų įstaiga (-os)

GR – Gyventojų registras

ĮR – Įgaliojimų registras

JADIS – Juridinių asmenų dalyvių informacinė sistema

JAR – Juridinių asmenų registras

KYC – principas „Pažink savo klientą“ (angl. *know your customer*)

NRVAR – Neveiksnių ir ribotai veiksnų asmenų registras

PEP – politiškai pažeidžiami (paveikiami) asmenys (angl. *politically exposed person*), kaip apibrėžta PPTFPI.

PPTFPI – Pinigų plovimo ir teroristų finansavimo prevencijos įstatymas

RC – VĮ Registrų centras

## Santrauka

2018 m. Mokėjimų taryba<sup>1</sup> sukūrė Kliento pažinimo (KYC) proceso optimizavimo užduoties grupę (toliau – Grupė), kurios tikslas – išnagrinėti KYC informacijos surinkimo optimizavimo Lietuvoje galimybes ir pateikti rekomendacijas. Užduoties grupė išnagrinėjo esamą KYC procesą Lietuvoje, šiam procesui reikalingus duomenis ir jų šaltinius, teisinę bazę, užsienio šalių praktiką, identifikavo esamas problemas ir remdamasi analize parengė KYC proceso optimizavimo Lietuvoje rekomendacijas.

Grupė savo darbe apibrėžia ir atskiria kliento identifikavimo ir KYC proceso sąvokas (PPTFPĮ šie procesai nėra atskirti). Nagrinėdama KYC proceso optimizavimą Grupė daro prielaidą, kad FĮ visais atvejais jau yra sėkmingai identifikavusi klientą, kaip tai apibrėžta PPTFPĮ.

Pagrindinės Grupės nustatytos problemos KYC procese – duomenų dubliavimas, duomenų neprieinamumas, duomenų nekaupimas ir duomenų išsibarstymas skirtinguose valstybės registruose. Optimizuotas KYC procesas atneštų naudos visiems finansų rinkos dalyviams (klientams, FĮ ir valstybei) – paprastesnis, pigesnis, greitesnis procesas, efektyvesnė pinigų plovimo ir terorizmo finansavimo prevencija šalies mastu.

Atlikusi analizę Grupė padarė išvadą, kad didžioji dauguma KYC proceso metu FĮ renkamų duomenų yra universalūs duomenys, kurie yra saugomi valstybės registruose ir informacinėse sistemose, todėl optimizuotame sprendime Grupė orientuojasi į galimybes efektyviai panaudoti valstybės registrų ir informacinių sistemų duomenis. Šiandien FĮ turi galimybę naudotis dalimi valstybės registruose ir informacinėse sistemose saugomų duomenų, tačiau tinkamos techninės sąsajos nebuvimas, nepritaikyta kainodara ir dabartinis teisinis reguliavimas daro registruose saugomų duomenų naudojimą neefektyvų arba neprieinamą FĮ.

Grupė identifikavo kelis esminius dabartinio KYC proceso gerinimo (duomenų patikimumo ir prieinamumo didinimo bei klientų patirties gerinimo) aspektus:

1. **Galimybė įtvirtinti teisinį reguliavimą, leidžiantį** pagal PPTFPĮ reikalavimus identifikavus klientą FĮ **naudoti valstybės registrus ir informacines sistemas kaip pirminį šaltinį** kitiems KYC duomenims surinkti, **kad klientai tik patvirtintų duomenų teisingumą**. Dabartiniame PPTFPĮ yra įtvirtintas principas, kad kliento ir galutinio naudos gavėjo tapatybei nustatyti (įskaitant KYC procesą) reikiamus duomenis pirmiausia reikia gauti iš kliento, o paskui juos patikrinti patikimuose ir nepriklausomuose šaltiniuose. Tai reiškia, kad klientas pats FĮ privalo pateikti visus reikiamus duomenis, kuriuos vėliau FĮ pakartotinai pasiima iš valstybės registrų ir informacinių sistemų duomenims sutikrinti. Toks PPTFPĮ įtvirtintas kliento ir galutinio naudos gavėjo tapatybės nustatymo procesas nėra įtvirtintas ES direktyvose, tokio reikalavimo nėra ir kaimyninėse šalyse (Latvijoje, Estijoje). Grupė siūlo įtvirtinti teisinį reguliavimą, leidžiantį atvirkštinį procesą ir nesukeliantį nepagrįstų rizikų.
2. **Galimybė leisti FĮ savo nuožiūra, remiantis rizika pagrįstu vertinimu, nusistatyti atvejus, kai KYC duomenys gali būti atnaujinami nesikreipiant į klientą**. Grupė taip pat atkreipė dėmesį, kad pagal dabartinį Lietuvos banko išaiškinimą tiesioginis duomenų (dokumentų) gavimas iš patikimų ir nepriklausomų šaltinių laikytinas tinkamu kliento bei galutinio naudos gavėjo duomenų atnaujinimui dalykinių santykių metu, tačiau atnaujinti duomenys visais atvejais turi būti pateikiami klientui jų teisingumui patvirtinti ir (ar) jiems koreguoti ir papildyti. Grupės nuomone, toks reikalavimas nėra būtinas, nes pasitaiko atvejų, kai periodinio duomenų atnaujinimo metu FĮ nenustato jokių požymių, kad anksčiau kliento FĮ pateikti ir patvirtinti

<sup>1</sup> <https://www.lb.lt/lt/mokejimu-taryba>

duomenys pakito, o prašymas patvirtinti atnaujintus duomenis apsunkina klientą ir kartais, nepavykus susisiekti su klientu, apriboja kliento galimybes naudotis finansinėmis paslaugomis.

3. **Galimybė FĮ patikimame šaltinyje patikrinti, ar asmuo yra politiškai pažeidžiamas.** Šiuo metu informacija apie PEP yra fragmentuota ir kaupiama keliose skirtingose valstybinėse duomenų bazėse, tačiau ir ši informacija nėra išsami. Grupės nuomone, Lietuvoje turėtų būti sukurta PEP duomenų bazė, iš įvairių valstybės registų konsoliduojanti duomenis, reikalingus visiems PEP, kaip jie suprantami pagal PPTFPĮ, identifikuoti.
4. **Galimybė patikimai nustatyti galutinį naudos gavėją ir nuosavybės struktūrą juridinių asmenų KYC procese.** Tyrimo metu nustatyta, kad FĮ, siekdamos nustatyti galutinį naudos gavėją ir nuosavybės struktūrą, renka informaciją iš pačių klientų, tikrina JADIS, JAR (kiek informacija ten prieinama), tarptautines duomenų bazines bei kitus šaltinius. Tačiau, Grupės nuomone, tokiais būdais patikrinta informacija nėra visiškai patikima. Grupė skatina JADIS registro, kuriame būtų saugomi duomenys ir apie galutinius naudos gavėjus ir kliento nuosavybės struktūrą, kūrimą, taip pat JADIS integraciją su kitų valstybių registrais įgyvendinant AMLD5 reikalavimus.
5. **Galimybė gauti nepilnamečių gimimo liudijimo duomenis, o neveiksnių ar ribotai veikusių asmenų duomenis iš registų neprašant nepilnamečių, neveiksnių ar ribotai veikusių asmenų atstovų ar, tam tikrais atvejais, pačių klientų patiems pateikti ryšį patvirtinantį dokumentą.** Papildomai siekdama efektyvinti dalykinių santykių užmezgimą su nepilnamečiais, neveiksniais ar ribotai veiksniais asmenimis, Grupė atkreipia dėmesį į tai, kad rinkoje kai kurios FĮ yra suformavusios praktiką nedubliuoti atstovo tapatybės nustatymo tuo atveju, kai kliento tapatybę jau yra nustatyta pagal PPTFPĮ.

**Grupė, įvertinusi alternatyvių KYC procesų optimizavimo naudas ir grėsmes, siūlo optimizuoti KYC procesą panaudojant KYC API sprendimą.** KYC API sprendime nebūtų kuriama nauja duomenų bazė, nes reikiamus duomenis FĮ iš valstybės registų ir informacinių sistemų galėtų paimti per vieną langelį teikdama užklausą KYC API sprendimo valdytojui. Gautus atskiros KYC užklausos duomenis kiekviena FĮ saugotų individualiai.

Grupės nuomone, KYC API sprendimas turėtų būti „bazinė paslauga“, kuri padėtų išvengti skirtingo teisinės bazės interpretavimo ir kartu netrukdytų rinkoje kurtis privačioms iniciatyvoms, siūlančioms FĮ ne tik pagrindinių KYC duomenų ištraukimą iš valstybės registų ir informacinių sistemų, tačiau ir papildomų paslaugų.

Grupė KYC API sprendimą siūlo kurti naudojantis RC duomenimis, o naujai sukurtus registrus (pavyzdžiui, VTEK – dėl PEP arba RC – galutinių naudos gavėjų registrą) integruoti į tą patį sprendimą vėlesniuose etapuose. KYC API sprendimas ateityje galėtų būti derinamas su kitais užsienyje sukurtais panašiais sprendimais. Taip pat, Grupės nuomone, įgyvendinus KYC API sprendimą, ateityje būtų galima svarstyti sukurti naują centralizuotą duomenų, nelaikomų valstybės registruose ar informacinėse sistemose, bazę ir ją taip pat prijungti prie KYC API sprendimo. Tačiau galimybė prijungti centralizuotą duomenų bazę turėtų būti papildomai išnagrinėta, siekiant įvertinti visą iš to kylančią riziką ir naudą.

Sukūrus KYC API sprendimą FĮ gautų didžiąją dalį reikalingų KYC duomenų tiesiogiai iš patikimo ir nepriklausomo šaltinio, o tai prisidėtų prie finansinių paslaugų prieinamumo didinimo, informacijos patikimumo ir geresnės kliento patirties. Pažymėtina, kad, siekiant didžiausios KYC API sprendimo naudos, lygiagrečiai turėtų būti įtvirtintas teisinis reguliavimas, leidžiantis pagal PPTFPĮ reikalavimus identifikavus klientą FĮ naudoti valstybės registrus ir informacines sistemas kaip pirminį šaltinį.

Kadangi Grupės siūlomą KYC API sprendimą įgyvendinantis ir valdantis subjektas KYC duomenų nekaupytų (nauja duomenų bazė nebūtų kuriama) ir tvarkytų juos tik tiek, kiek reikia duomenims gauti iš viešųjų registrų ir informacinių sistemų ir perduoti FĮ bei kitiems įpareigotiesiems subjektams, modelio įgyvendinimo tikslais būtų efektyviausia, jei modelį įgyvendinantis subjektas neįgytų duomenų valdytojo statuso ir veiktų kaip viešųjų registrų duomenų tvarkytojas.

1 lentelė. Grupės suformuluotos rekomendacijos kitoms institucijoms dėl KYC proceso optimizavimo Lietuvoje

<b>Institucija</b>	<b>Rekomendacija</b>
VĮ Registrų centrai	<p>1. Sparčiau tobulinti JADIS vystymą, užtikrinti, kad šioje informacinėje sistemoje kaupiami duomenys būtų tikslūs ir aktualūs, sudaryti galimybę vienos užklausos metu gauti informaciją ne tik apie akcininkus, bet ir apie galutinius naudos gavėjus ir kliento nuosavybės struktūrą, taip pat užtikrinti galimybę gauti duomenis iš kitų Europos Sąjungos valstybių narių, įgyvendinant AMLD5 reikalavimus.</p> <p>2. RC skatinamas peržiūrėti savo duomenų kainodarą, kuri šiuo metu neskatina efektyvesnio elektroninio duomenų naudojimo.</p>
Lietuvos bankui	<p>1. Kol PPTFPĮ bus numatyta tokia galimybė, kliento ir galutinio naudos gavėjo duomenų atnaujinimo metu leisti FĮ savo nuožiūra, remiantis rizika pagrįstu vertinimu, nusistatyti atvejus, kai:</p> <p>a) duomenų teisingumui patvirtinti ir (arba) jiems koreguoti ir papildyti būtina kreiptis į klientą (pavyzdžiui, tokiu atveju, kai patikimuose ir nepriklausomuose šaltiniuose nustatytas dalyvių pasikeitimas, o klientas apie tokį pasikeitimą nebuvo informavęs FĮ);</p> <p>b) duomenys gali būti atnaujinami nesikreipiant į klientą (pavyzdžiui, kai periodinio duomenų atnaujinimo metu nenustatoma jokių pokyčių tarp kliento anksčiau FĮ pateiktų duomenų bei duomenų atnaujinimo metu patikimuose ir nepriklausomuose šaltiniuose esančių duomenų).</p>
Finansinių nusikaltimų tyrimo tarnybai prie Vidaus reikalų ministerijos	<p>1. Koreguoti PPTFPĮ ir sudaryti galimybę FĮ naudoti duomenis (dokumentus), gautus tiesiogiai iš patikimų ir nepriklausomų šaltinių, dalykinių santykių užmezgimo metu. Svarbu pabrėžti, kad visais atvejais prieš naudojant duomenis (dokumentus), gautus tiesiogiai iš patikimų ir nepriklausomų šaltinių, FĮ identifikuotą klientą (fizinį asmenį) arba kliento (fizinio ar juridinio asmens) atstovą (fizinį asmenį) remiantis asmens tapatybę patvirtinančiu dokumentu asmeniui dalyvaujant fiziškai ar kitais PPTFPĮ 11 straipsnyje numatytais nuotolinio identifikavimo būdais. Identifikavus klientą (fizinį asmenį) arba kliento (fizinio ar juridinio asmens) atstovą (fizinį asmenį), FĮ kitus duomenis (dokumentus), reikalingus kliento ir galutinio naudos gavėjo tapatybei nustatyti (pavyzdžiui, duomenis apie juridinio asmens vadovus, dalyvius, galutinius naudos gavėjus), tiesiogiai gautų iš patikimų ir nepriklausomų šaltinių ir pateiktų klientui ar jo atstovui patvirtinti duomenų teisingumą ir (ar) juos koreguoti, papildyti.</p>
Vidaus reikalų ministerijai	<p>1. Įvertinti galimybes sukurti naują valstybinę PEP duomenų bazę arba pavesti jau esamiems registrams praplėsti duomenų kiekį taip, kad</p>

	vieno langelio principu FĮ galėtų patikrinti, ar asmuo yra PEP.
VĮ Registrų centrui, Ekonomikos ir inovacijų ministerijai	Galimo KYC API sprendimo valdytoju būti valstybės institucijai. Daugumos grupės narių nuomone, tinkamiausias valdytojas būtų RC.

### **Esminės rekomendacijos KYC API sprendimo valdytojui:**

1. KYC API sprendimas turi būti paremtas vieno langelio principu – tai reiškia, kad nesvarbu, kiek valstybės registrų ir (arba) informacinių sistemų egzistuoja Lietuvoje KYC duomenims surinkti, FĮ teiktų tik vieną užklausą KYC API sprendimo valdytojui ir gautų visus reikiamus duomenis, reikalingus KYC procesui optimizuoti. Sprendimo valdytojas būtų atsakingas už tinkamą integraciją su visais reikalingais valstybės registrais ir informacinėmis sistemomis, pats atnaujintų techninius sprendimus ir aprašymus tada, kai registrų duomenys ar sąsajos būtų atnaujinti. Labai svarbu, kad FĮ galėtų pasirašyti sutartį tik su tokio sprendimo valdytoju.

2. Kuriamas KYC API sprendimas turėtų būti „bazinė paslauga“, kuri netrukdytų rinkoje kurtis privačioms iniciatyvoms, siūlančioms FĮ ne tik pagrindinių KYC duomenų ištraukimą iš valstybės registrų ir informacinių sistemų, bet ir papildomų paslaugų.

3. Įgyvendinus KYC API sprendimą, būtų siūloma apsvarstyti galimybę dalį KYC anketinių duomenų, kurie nesaugomi valstybės registruose ar informacinėse sistemose, saugoti atskiroje duomenų bazėje, kuri galėtų būti prijungta prie KYC API sąsajos. Tokie duomenys galėtų būti arba FĮ kliento pateikti individualūs duomenys, arba mažesnio patikimumo, palyginti su valstybės registrais ir informacinėmis sistemomis, duomenys, gaunami iš kitų įstaigų (telefono numeris, saugomas pas mobiliųjų tinklų operatorių). Mažesnio patikimumo lygio duomenys reikalingi tarptautiniam KYC sprendimui ir tada, kai valstybės registrų ir informacinių sistemų duomenys per brangūs arba neprieinami. Norint toliau plėtoti idėją, reikia papildomos analizės, taip pat įvertinti EK Ekspertų darbo grupės dėl el. atpažinties ir nuotolinių KYC procesų naujausius priimtus sprendimus.

4. KYC API sprendimas turi būti atviras tarptautinei rinkai – techninis sprendimas turi būti įgyvendintas taip, kad užklausų teikėjai (FĮ) nebūtų apribojami pagal įsisteigimo šalį. Jei užsienio šalies FĮ pasirašytų duomenų gavimo sutartį su KYC API sprendimo valdytoju ir integruotų Lietuvos duomenų valdytojo techninius sprendimus, tada užsienio FĮ galėtų tapti sprendimo dalyviu. Taip pat svarbu, kad sąsajos techninis sprendimas informacinių technologijų požiūriu būtų taip suprojektuotas ir suprogramuotas, kad užklausa galėtų būti pateikiama užsienio analogiškos sąsajos arba „centralizuoto“ KYC sprendimo valdytojui, t. y. numatyti, kad užklausa galėtų būti siunčiama ne tik Lietuvos, bet ir užsienio valstybių registrams ar užsienio analogiškų KYC schemų valdytojams.

## 1. KYC proceso sąvoka




PPTFPĮ ir su juo susijusiuose poįstatyminiuose aktuose FĮ ir kitiems įpareigotiesiems subjektams yra numatyta pareiga imtis prevencinių priemonių siekiant užkirsti kelią pinigų plovimui ir teroristų finansavimui, tinkamai nustatoma kliento ir galutinio naudos gavėjo tapatybė bei naujų ir esamų klientų atžvilgiu įgyvendinamas principas „Pažink savo klientą“ (angl. *Know your customer*, KYC). Šis principas reiškia, kad FĮ turi surinkti pakankamai informacijos norėdamos suprasti, kas yra jų klientas, kokia veikla jis užsiima, ir užtikrinti, kad kliento atliekamos operacijos atitinka jo vykdomos ekonominės veiklos sritį ir apimtį.

Atkreiptinas dėmesys į tai, kad PPTFPĮ neišskiria kliento tapatybės identifikavimo (angl. *identification*), patikrinimo (angl. *verification*) ar kliento pažinimo (angl. *know your customer*) kaip atskirų procesų (visa tai vadinama kliento ir naudos gavėjo tapatybės nustatymu), tačiau, Grupės nuomone, svarbu atskirti ir FĮ bei priežiūros institucijoms vienodai suprasti šiuos procesus siekiant optimizuoti KYC procesą.

KYC procesą FĮ gali pradėti po to, kai įvykdomas kliento identifikavimas (žr. 1 pav.). Grupės nuomone, kliento identifikavimas susideda iš dviejų žingsnių. Pirmasis žingsnis yra: 1) fizinio asmens atveju – jo vardo, pavardės ir asmens kodo gavimas; 2) juridinio asmens atveju – atstovo (fizinio asmens) vardo, pavardės ir asmens kodo, taip pat įmonės pavadinimo bei įmonės kodo gavimas. Antrasis identifikavimo žingsnis yra gautų duomenų patikrinimas. Klientui dalyvaujant fiziškai, vykdydama kliento pateiktų duomenų patikrinimą, FĮ privalo gauti kliento, fizinio asmens arba juridinio asmens atstovo, asmens tapatybę patvirtinantį dokumentą ir (arba) atstovavimo pagrindą. Klientui užmezgant dalykinius santykius nuotoliniu būdu, FĮ tikrina kliento pateiktus identifikacinius duomenis vadovaudamasi PPTFPĮ 11 straipsnio reikalavimais.

Grupė savo analizėje nagrinėja, kaip FĮ gali efektyviau įgyvendinti KYC duomenų surinkimą, t. y. gauti duomenis, dokumentus ar informaciją, reikalingą pagal PPTFPĮ 9, 10 ir 12 straipsnius. Nagrinėdama KYC proceso optimizavimą, Grupė daro prielaidą, kad FĮ visais atvejais jau yra sėkmingai identifikavusi klientą, kaip apibrėžta pirmiau. Užduoties grupė savo tyrime orientuojasi į mokėjimo paslaugas teikiančių FĮ poreikius, tačiau, įvertinus tai, kad ir kitoms FĮ optimizuotas KYC sprendimas gali būti aktualus, užduoties grupė nagrinės visas FĮ.

1 pav. Kliento ir naudos gavėjo tapatybės nustatymas

Kliento ir naudos gavėjo tapatybės nustatymas		
Identifikavimas	KYC duomenų surinkimas	Stebėjimas
FĮ gauna ir patikrina duomenis klientui dalyvaujant fiziškai arba nuotoliniu būdu 	<b>KYC grupė šioje studijoje nagrinėja FĮ galimybes surinkti informaciją pagal PPTFPĮ 9, 10 ir 12 straipsnius</b>	
FA atveju:  vardą, pavardę, asmens kodą JA atveju:  atstovo v. pavardę, asmens kodą, atstovavimo pagrindą; įmonės pavadinimą, įmonės kodą		

**Grupės pozicija.** Nors PPTFPI vartojama viena sąvoka „kliento ir naudos gavėjo tapatybės nustatymas“, svarstant KYC proceso optimizavimo klausimą, svarbu atskirti ir vienodai FĮ bei priežiūros institucijoms suprasti kliento identifikavimo ir KYC procesus. Grupė savo analizėje nagrinėja KYC duomenų surinkimo, atliekamo sėkmingai identifikavus klientą, optimizavimą.

## 2. Esamo KYC proceso problematika ir optimizavimo nauda

Griežtėjant reguliavimui, FĮ vis daugiau išteklių turi skirti KYC reikalavimams įgyvendinti, tai trukdo mažinti finansinių paslaugų kainas galutiniams vartotojams ar net turi įtakos jų brangimui. „Thomson Reuters“ atlikto tyrimo<sup>2</sup> duomenimis, kliento registravimo (angl. *onboarding*) laikas FĮ 2016 m. išaugo net 22 proc., 2017 m. – dar 16 proc. ir tikėtina, kad dėl AMLD5 perkėlimo į nacionalinę teisę artimiausiu metu augs ir toliau.

Šiuo metu FĮ klientai, ypač įmonės, norėdami pradėti naudotis FĮ paslaugomis arba atnaujindami informaciją apie save, turi pateikti visus KYC procesui reikalingus duomenis kiekvienai FĮ, kurios paslaugomis naudojasi. Taip pat didžioji dalis klientų KYC procese pateikiamų duomenų jau yra saugomi įvairiuose valstybės registruose ar kituose patikimuose duomenų šaltiniuose, šią informaciją FĮ taip pat turi gauti norėdamos patikrinti kliento pateiktus duomenis. Didelis turimų pateikti duomenų kiekis kiekvienai FĮ apsunkina klientų naudojimąsi finansinėmis paslaugomis, sukuria papildomų kaštų, ypač įmonėms.

FĮ, atlikdamos KYC procesą, susiduria ir su duomenų gavimo, kokybės bei kainos problema. Ne visi valstybės registruose ir informacinėse sistemose saugomi bei KYC procesui reikalingi duomenys yra prieinami FĮ, dažnai duomenys saugomi nesistemiškai ar nėra tinkamai sugrupuoti, todėl FĮ reikalauja, kad šiuos duomenis pateiktų patys klientai. Kita problema – šiuo metu Lietuvoje nėra PEP duomenų bazės, todėl FĮ negali būti visiškai tikra, ar asmuo, norintis pradėti dalykinius santykius, nėra PEP. Atkreipiame dėmesį, kad PEP identifikavimas yra svarbus valstybei. Nors kai kurie duomenys yra saugomi valstybės registruose, tačiau jų gavimo kaina yra neproporcingai didelė.

2 lentelė. Pagrindinės grupės identifikuotos problemos KYC procese

<b>Duomenų dubliavimas</b>	Reikalavimas klientams prieš pradėdant naudotis FĮ paslaugomis pildyti tuos duomenis, kurie jau yra valstybės registruose ir (arba) informacinėse sistemose ir yra papildomai gaunami FĮ, siekiant patikrinti kliento pateiktus duomenis. Tai vienas neefektyviausių reikalavimų.
<b>Duomenų neprieinamumas</b>	FĮ kai kuriuos duomenis renka rankiniu būdu, nors jie jau yra valstybės registruose ir (arba) informacinėse sistemose, tačiau nėra prieinami FĮ dėl teisinio reguliavimo arba dėl automatinio būdo duomenims pateikti trūkumo.
<b>Duomenų nekaupimas</b>	Pavyzdžiui, JADIS nekaupia galutinio naudos gavėjo informacijos ir įmonės nuosavybės bei struktūrinės schemas. Valstybės registruose nėra kaupiama dalis duomenų apie PEP asmenis.
<b>Duomenų išsibarstymas skirtinguose registruose</b>	Pavyzdžiui, informacija apie PEP asmenis.

<sup>2</sup> *Cost of Compliance 2017*, apklausta 900 FĮ daugelyje pasaulio šalių  
<https://legal.thomsonreuters.com/en/insights/reports/cost-compliance-2017>



Optimizuotas KYC procesas leistų tiek FĮ, tiek klientams sutaupyti išteklių ir lėšų, skiriamų KYC reikalavimams įgyvendinti, kurie būtini norint naudotis finansinėmis paslaugomis. Paprastesnis ir mažiau išteklių reikalaujantis procesas stiprintų konkurenciją tarp FĮ teikiant finansines paslaugas ir klientų įtrauktį naudojantis finansinėmis paslaugomis. Efektyvesnis valstybės duomenų panaudojimas stiprintų valstybės santykį su FĮ, gerintų KYC procesui reikalingų duomenų kokybę ir efektyviau užtikrintų pinigų plovimo ir terorizmo finansavimo prevenciją šalyje.

3 lentelė. KYC proceso optimizavimo nauda

<b>FĮ klientas (fizinis asmuo ar įmonė)</b>	Paprastesnis naudojimas FĮ paslaugomis, didesnė įtrauktis finansų rinkoje, tikslesni duomenys apie klientą ir efektyvesnis duomenų atnaujinimas. Klientai sutaupytų laiko pateikdami ir tvirtindami duomenis (dabartinė FĮ praktika rodo, kad dažnai klientams sunku suprasti, kokius konkrečiai duomenis reikia pateikti FĮ, todėl vyksta pakartotiniai kreipimaisi į klientus prašant ištaisyti klaidas ar pateikti papildomą informaciją).
<b>Valstybė</b>	Geresnis kaupiamų duomenų administravimas, duomenų kokybės užtikrinimas, efektyvesnis bendradarbiavimas su FĮ pinigų plovimo ir terorizmo finansavimo prevencijos kontekste, paprastesnis FĮ tikrinimas.
<b>FĮ</b>	KYC procesas taptų efektyvesnis, mažesni kaštai, sumažėjusi rizika, kad klientas nesinaudos FĮ paslaugomis dėl per sudėtingo KYC proceso, didesnė konkurencija, lengvesnis santykio su nauju klientu užmezgimas, išaugusi galimybė naudotis patikimiausiais duomenimis (t. y. valstybės registrais).

**Grupės pozicija.** KYC procese identifikuotos problemos: duomenų dubliavimas, duomenų neprieinamumas, duomenų nekaupimas ir duomenų išsibarstymas skirtinguose valstybės registruose. KYC proceso optimizavimas būtų naudingas FĮ klientams, valstybei ir FĮ.

### 3. KYC proceso duomenys

Grupė atkreipia dėmesį, kad KYC procesas skiriasi atsižvelgiant į tai, kas ketina pasinaudoti finansinėmis paslaugomis: fizinis asmuo ar juridinis asmuo, rezidentas ar ne rezidentas. Atsižvelgdama į klausimo FĮ aktualumą ir siekdama koncentruoto ir rezultatyvaus tyrimo, Grupė sutarė, kad tyrime bus nagrinėjamas fizinių asmenų rezidentų ir juridinių asmenų rezidentų KYC procesas. Grupė nenagrinės ne rezidentų KYC proceso, tam reikia išsamesnės analizės.

Nagrinėjant fizinių ar juridinių asmenų KYC duomenis, svarbus universalių ir individualių duomenų atskyrimas. Tai reiškia, kad surinkus universalią informaciją apie fizinį ar juridinį asmenį iš valstybės registru ir informacinių sistemų, FĮ papildomai renka individualią informaciją apie klientą, susijusią su konkrečiomis paslaugomis, kuriomis klientas ketina naudotis FĮ, taip pat bet kurią kitą informaciją apie klientą, kuri FĮ yra būtina. Atsižvelgiant į tai, kad KYC centralizuotas sprendimas yra galimas tik dėl universalių duomenų, taip pat atsižvelgiant į pagrindinius asmens duomenų tvarkymo principus, t. y. tikslo apribojimo principą (kad duomenys būtų renkami tik pinigų plovimo ir terorizmo finansavimo prevencijos tikslais, atsižvelgiant į finansinės paslaugos pobūdį) ir duomenų kiekio mažinimo principą (kad duomenų būtų renkama tik tiek, kiek yra būtina numatytiems tikslams

pasiekti), Grupės tyrimas orientuotas tik į universalius duomenis t. y. tuos, kuriuos FĮ gali surinkti iš valstybės registrų ir kitų patikimų duomenų šaltinių.

Vadovaujantis teisės aktais ir FĮ praktika, sudarytas sąrašas duomenų, kuriuos FĮ, atlikdama KYC, renka KYC tikslais (žr. 4 lentelę). Grupė KYC proceso metu renkamų duomenų sąrašė taip pat atspindėjo esamus duomenų šaltinius, taip pat galimus duomenų šaltinius, iš kurių FĮ galėtų gauti tam tikrus duomenis optimizavus KYC procesą (žr. 1 priedą).

4 lentelė. KYC proceso metu renkami duomenys

	<b>Fizinis asmuo</b>	<b>Juridinis asmuo</b>
<b>Identifikavimas</b>	<ul style="list-style-type: none"> <li>▪ Vardas, pavardė, asmens kodas</li> </ul>	<ul style="list-style-type: none"> <li>▪ Juridinio asmens pavadinimas, kodas</li> </ul> <p><b>Atstovas:</b></p> <ul style="list-style-type: none"> <li>▪ Vardas, pavardė, asmens kodas (gimimo data)</li> <li>▪ Atstovavimo pagrindą pagrindžiantis dokumentas ir duomenys, pagal kuriuos jis patikrinamas</li> </ul>
<b>KYC universalūs duomenys</b>	<ul style="list-style-type: none"> <li>▪ Asmens dokumento (arba leidimo gyventi Lietuvos Respublikoje) numeris, išdavimo ir galiojimo data, išdavimo vieta</li> <li>▪ Pilietybė</li> <li>▪ Nuotrauka</li> <li>▪ Parašas</li> <li>▪ Ar asmuo yra PEP? Jeigu taip: vardas, pavardė, einamos pareigos, institucija, ryšys su klientu.</li> <li>▪ Lėšų šaltinis</li> <li>▪ Gyvenamoji vieta</li> <li>▪ Kontaktiniai duomenys</li> <li>▪ Ar klientui, jo atstovui ar galutiniam naudos gavėjui taikomos finansinės sankcijos?</li> </ul>	<ul style="list-style-type: none"> <li>▪ Teisinė forma</li> <li>▪ Registruota buveinė</li> <li>▪ Faktinė buveinė</li> <li>▪ Registracijos išrašas, jo išdavimo data</li> <li>▪ Valdymo struktūra</li> <li>▪ Veiklos pobūdis</li> <li>▪ Ar vadovas, naudos gavėjas yra PEP? Jeigu taip, to asmens vardas, pavardė, einamos pareigos, institucija, ryšys su klientu.</li> <li>▪ Ar klientui, jo vadovui, galutiniam naudos gavėjui ar atstovui taikomos finansinės sankcijos?</li> <li>▪ Lėšų šaltinis</li> <li>▪ Kontaktiniai duomenys</li> </ul> <p><b>Atstovas:</b></p> <ul style="list-style-type: none"> <li>▪ Atstovo asmens dokumento (arba leidimo gyventi Lietuvos Respublikoje) numeris, išdavimo ir galiojimo data, išdavimo vieta</li> <li>▪ Atstovo pilietybė</li> <li>▪ Atstovo nuotrauka</li> <li>▪ Atstovo parašas</li> </ul> <p><b>Vadovas:</b></p> <ul style="list-style-type: none"> <li>▪ Vardas, pavardė</li> <li>▪ Asmens kodas arba gimimo data</li> <li>▪ Pilietybė</li> </ul> <p><b>Naudos gavėjai:</b></p> <ul style="list-style-type: none"> <li>▪ Vardas, pavardė,</li> <li>▪ Asmens kodas arba gimimo data,</li> <li>▪ Pilietybė</li> </ul>
<b>KYC individualūs duomenys</b>	<ul style="list-style-type: none"> <li>▪ Ar klientas pats naudosis FĮ paslaugomis?</li> <li>▪ Išmokos gavėjas (tik gyvybės draudimo)</li> <li>▪ Dalykinių santykių tikslas ir pobūdis</li> <li>▪ Lėšų šaltinis</li> <li>▪ Turto šaltinis (tam tikrais atvejais)</li> </ul>	<ul style="list-style-type: none"> <li>▪ Ar klientas pats naudosis FĮ paslaugomis?</li> <li>▪ Dalykinių santykių tikslas ir pobūdis</li> <li>▪ Lėšų šaltinis</li> <li>▪ Turto šaltinis (tam tikrais atvejais)</li> </ul>

**Grupės pozicija.** Grupės nuomone, absoliuti dauguma KYC proceso metu renkamų duomenų yra universalūs duomenys, kurie gali būti gaunami iš pirminių patikimų šaltinių (valstybės registru ir informacinių sistemų), todėl optimizuotame sprendime Grupė orientuojasi į universalius duomenis ir valstybės registru ir informacinių sistemų duomenų panaudojamumą.

#### **4. Valstybės registru duomenų panaudojamumas KYC procese**

Grupė nustatė, kad dauguma duomenų, reikalingų KYC įgyvendinti, yra universalūs (žr. 4 lentelę) ir kad dauguma šių duomenų yra renkami ir saugomi valstybės registruose ir (arba) informacinėse sistemose (žr. 1 priedą). Todėl efektyvinant KYC procesus pirmiausia turėtų būti siekiama užtikrinti efektyvų ir didžiausią galimą duomenų iš valstybės registru ir (arba) informacinių sistemų panaudojimą. Siekdama įvertinti galimybes panaudoti valstybės registruose ir duomenų bazėse saugomus KYC reikiamus duomenis, Grupė susitiko su Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos (nuo 2018 m. spalio 2 d. – prie Ekonomikos ir inovacijų ministerijos) (toliau – IVPK), Vyriausiosios tarnybinės etikos komisijos (toliau – VTEK), RC ir Valstybinės mokesčių inspekcijos (toliau – VMI) atstovais, nagrinėjo Lietuvos Respublikos vyriausiosios rinkimų komisijos (toliau – VRK) duomenis, siekdama suprasti:

- šių institucijų teikiamą (turimą) informaciją apie fizinius ir juridinius asmenis, reikalingą FĮ identifikuojant klientus ir vykdant KYC;
- galimybes (įskaitant reikiamus teisinės bazės pakeitimus) ateityje FĮ gauti informaciją apie fizinius ir juridinius asmenis per vieną kanalą iš valstybės registru ir duomenų bazių.

##### **4.1. Galimybės surinkti registru duomenis vieno langelio principu**

###### IVPK

Technologiškai IVPK yra sukūręs prieigą prie valstybės registru (toliau – IVPK hub), kuri veikia vieno langelio principu, tačiau šiuo metu IVPK hub neapima visų valstybės registru ir informacinių sistemų, kuriose saugomi KYC procesui reikalingi duomenys. Pagal šiandienos teisinę bazę IVPK hub paslaugomis gali naudotis tik viešasis sektorius, tad, norint FĮ naudotis IVPK hub paslaugomis, ši teisė turi būti numatyta įstatymuose, pvz., Valstybės informacinių išteklių valdymo įstatyme. Taip pat teisiniai duomenų gavimo klausimai turi būti sprendžiami tarp konkretaus registro ir duomenų gavėjo individualiai. Papildomai būtų reikalingi technologiniai pokyčiai kuriant KYC procesui pritaikytą duomenų pateikimo paslaugą.

###### RC

RC turi platų paslaugų teikimo spektrą savo klientams (įskatinat FĮ), visišką e. integraciją su pagrindiniais valstybės registrais ir informacinėmis sistemomis (JAR, NTR, GR ir kt.). RC taip pat yra sukūręs atvirą e. paslaugų kūrimo platformą, kurioje galima sujungti ir analizuoti skirtingų registru ar informacinių sistemų duomenis, sukūrus aplikaciją juos pateikti pagal kliento poreikius. Paslauga skirta naudotis tiek privatiems, tiek instituciniams klientams.

FĮ naudojasi RC duomenimis, tačiau ieškoma patogesnio duomenų paėmimo būdo. Taip pat pažymėtina, kad FĮ ir jų galimybės šiuo metu gauti visus reikiamus duomenis iš RC yra gana skirtingos dėl teisės aktų aiškinimo, organizacinių, techninių priežasčių (buvo atvejų, kai FĮ kilo sunkumų norint gauti kliento nuotrauką). Šiuo metu FĮ naudojasi standartinėmis RC paslaugomis, kurios nesudaro patogių techninių galimybių FĮ pasiimti reikiamus duomenis, taip pat kainodaros prasme, RC apmokestina visą pateikiamo registro duomenų apimtį, nors FĮ reikia tik dalies duomenų.

FĮ gali naudotis RC sukurta nauja e. paslaugų kūrimo platforma, tačiau, norint gauti personalizuotus duomenis pagal konkrečią užklausą, reikia sukurti specifinę sąsają – efektyviausia ją kurti rinkos mastu. RC duomenys kainuoja, todėl sukurtas įrankis gali padėti sumažinti kaštus, nes ištraukiamas tik reikalingų duomenų kiekis, o ne visas duomenų masyvas. RC šiuo metu peržiūri kainodarą. Taip pat specializuota paslauga būtų sukurta ir pritaikyta FĮ poreikiams KYC srityje, todėl ji galėtų užtikrinti vienodas galimybes visiems FĮ gauti visus joms KYC tikslais reikiamus duomenis vienodomis sąlygomis, tai mažintų FĮ atėjimo į rinką barjerus.

Grupės nariai pažymėjo, kad ypač svarbu, kas būtų aplikacijos prie RC e. duomenų platformos valdytojas, t. y. ar valdytojas yra RC, ar perkama paslauga iš trečiosios šalies. Aplikacijos valdytojas turi prižiūrėti ir atlikti pakeitimus savo aplikacijoje. Taip pat aplikacijos valdytojas prisiima atsakomybę už paslaugos tinkamumą.

**Grupės pozicija.** KYC reikalavimams įgyvendinti visos FĮ renka ir naudoja tuos pačius universalius klientų duomenis. Didžioji dalis KYC reikiamų duomenų (universalūs duomenys) yra kaupiami valstybės registruose ir (arba) informacinėse sistemose, todėl, siekiant optimizuoti KYC procesą, pirmiausia turi būti užtikrinamas efektyvus ir patogus duomenų pernaudojimas. Dauguma valstybės registrų ir informacinių sistemų duomenų yra prieinami per RC, kuris teikia duomenis FĮ, tačiau, norint patogiai paimti duomenis, reikia naujo įrankio, kuris veiktų vieno langelio principu. Įrankio sukūrimas padėtų išvengti ir skirtingo teisinės bazės interpretavimo dėl galimybės FĮ naudoti valstybės registrų duomenis. Grupė taip pat skatina RC peržiūrėti savo duomenų kainodarą, kuri neskatina efektyvesnio elektroninio duomenų naudojimo.

#### **4.2. Problematika, susijusi su PEP**

KYC procese privaloma identifikuoti PEP. FĮ, siekdamos įgyvendinti šį reikalavimą, renka informaciją iš pačių klientų arba įvairių valstybinių ir komercinių duomenų bazių, tačiau Grupė nustatė, kad šiuo metu konsoliduotos PEP duomenų bazės nėra: nors tam tikra informacija apie PEP yra pasiekama keliose skirtingose valstybinėse duomenų bazėse, ši informacija nėra išsami ir neleidžia identifikuoti visų PEP, kaip jie suprantami pagal PPTFPĮ (žr. 2 priedą). Pavyzdžiui, VTEK informacinių duomenų sistema yra privačių interesų deklaracijos bazė, tai nėra PEP duomenų bazės atitikmuo. Politiškai pažeidžiamam asmeniui nėra privaloma privačių interesų deklaracijoje pateikti savo artimųjų duomenis.

VMI kaupia informaciją apie kai kuriuos PEP ir jų šeimos narius, nes šie asmenys privalo užpildyti metinę gyventojų (šeimos) turto deklaracijos formą FR001. Asmenys, turintys pildyti FR001 deklaracijos formą, apibrėžti Gyventojų turto deklaravimo įstatyme, tačiau PPTFPĮ politiškai pažeidžiamo asmens sąvoka yra platesnė nei minėto įstatymo. Šiuo metu VMI neturi teisinio pagrindo perduoti duomenis FĮ.

VRK turi politinių partijų kandidatų ir laimėjusių asmenų sąrašus, todėl jų informacija apie PEP asmenis yra tikslesnė, tačiau nerenkama informacija apie šeimos narius.

Svarstylini ir alternatyvūs informacijos, ar asmuo yra laikomas PEP, šaltiniai, pvz., Valstybinio socialinio draudimo fondo valdyba prie Socialinės apsaugos ir darbo ministerijos (toliau – SODRA), tačiau tam reikia išsamesnės analizės.

**Grupės rekomendacija.** Galimybė FĮ patikimame šaltinyje patikrinti, ar asmuo yra PEP, kaip tai suprantama pagal PPTFI, yra vienas esminių KYC proceso gerinimo aspektų. Grupės nuomone, Vidaus reikalų ministerija turėtų įvertinti galimybes sukurti naują valstybinę PEP duomenų bazę arba pavesti jau esamiems registrams praplėsti duomenų kiekį taip, kad vieno langelio principu FĮ galėtų patikrinti, ar asmuo yra PEP.

### 4.3. Problematika, susijusi su JADIS

Juridinių asmenų KYC procese nustatyti galutinį naudos gavėją ir nuosavybės struktūrą yra vienas svarbiausių uždavinių. Tyrimo metu nustatyta, kad FĮ, siekdamos nustatyti galutinį naudos gavėją ir nuosavybės struktūrą, skiria daug išteklių, renka informaciją iš pačių klientų, tikrina JADIS, JAR (kiek informacija ten prieinama), tarptautines duomenų bazines, kitus šaltinius, tačiau negali būti užtikrintos, kad tai gali būti laikoma patikimu ir nepriklausomu šaltiniu PPTFPI prasme. FĮ nuomone, tokiais būdais surinkta informacija nėra visiškai patikima.

Atkreiptinas dėmesys ir į tai, kad su dar didesnėmis problemomis susiduria FĮ, kurių klientų juridinių asmenų akcininkai yra kiti juridiniai asmenys arba užsienyje įsteigti juridiniai asmenys. Esminė šios problemos priežastis, kad nei ES, nei nacionaliniu lygmeniu nėra sukurto galutinių naudos gavėjų registro. Tai reiškia, kad pirmuoju atveju FĮ, gavusi informaciją, kad kliento juridinio asmens akcininkas yra kitas juridinis asmuo, privalo atlikti atskirą užklausą registre, ir dažnai ne vieną, norėdama nustatyti galutinį naudos gavėją.

Antruoju atveju, kai FĮ nustato, kad kliento juridinio asmens akcininkas yra užsienio valstybėje įsteigtas juridinis asmuo, FĮ, turėdama prievolę nustatyti galutinį naudos gavėją, naudojami jai prieinamais užsienio valstybių registrais ir kitais šaltiniais, kurių patikimumu nėra visiškai užtikrintos. Atsižvelgiant į tai, reikalavimas surinkti duomenis apie galutinius naudos gavėjus bei nuosavybės struktūrą, kai kliento akcininkai yra kiti juridiniai asmenys arba užsienyje įsteigti juridiniai asmenys, FĮ yra ypač sunkiai įgyvendinamas.

Pažymėtina, kad Europos Tarybos Ekspertų komiteto dėl priemonių, nukreiptų kovai su pinigų plovimu bei teroristų finansavimu (MONEYVAL) 2018 m. birželio 12 d. ataskaitoje<sup>3</sup> nurodoma, kad informacija apie juridinių asmenų galutinius naudos gavėjus labiausiai prieinama JAR ir JADIS, kurie kartu saugo informaciją apie 83,8 proc. Lietuvoje registruotų juridinių asmenų. Vis dėlto informacijos apie 16,2 proc. Lietuvoje registruotų juridinių asmenų galutinius naudos gavėjus nepateikia joks registras. Be to, ataskaitoje pabrėžiama, kad JADIS nėra įdiegtos informacijos tikrinimo sistemos, todėl nėra užtikrinama, kad šioje informacinėje sistemoje kaupiama informacija yra tiksli ir aktuali. Atsižvelgiant į tai, darytina išvada, kad šiuo metu FĮ neturi objektyvių galimybių iš patikimų ir nepriklausomų šaltinių nustatyti klientų juridinių asmenų galutinių naudos gavėjų ir nuosavybės struktūrą, kas yra laikoma esmiu klausimu atliekant juridinių asmenų KYC.

Grupės nuomone, informacinė sistema JADIS galėtų tapti konsoliduotu galutinių naudos gavėjų ir nuosavybės struktūros duomenų šaltiniu ir tapti pagrindine informacine sistema atliekant juridinių asmenų KYC. Šiuo tikslu turėtų būti paspartintas JADIS kūrimas, be to, JADIS vienos užklausos metu turėtų pateikti informaciją tiek apie akcininkus, tiek apie galutinius naudos gavėjus ir nuosavybės struktūrą. Problema, susijusi su klientų juridinių asmenų akcininkų, kai jie yra užsienio subjektai, KYC procesu galėtų būti dalinai išspręsta įgyvendinant ES AMLD5, kurioje yra numatytas reikalavimas sukurti bendrą galutinių naudos gavėjų duomenų bazę ES lygmeniu.

<sup>3</sup> <<https://rm.coe.int/committee-of-experts-on-the-evaluation-of-anti-money-laundering-measur/16809247ed>>

**Grupės rekomendacija.** RC paspartinti JADIS tobulinimą ir užtikrinti, kad šioje informacinėje sistemoje kaupiami duomenys būtų tikslūs ir aktualūs; sudaryti galimybę vienos užklauso metu gauti informaciją ne tik apie akcininkus, bet ir apie galutinius naudos gavėjus bei kliento nuosavybės struktūrą; sudaryti galimybę gauti duomenis iš kitų ES valstybių narių, įgyvendinant AMLD5 direktyvos reikalavimus.

## 5. KYC proceso optimizavimo alternatyvos, kitų šalių patirtis

### 5.1. KYC proceso optimizavimo alternatyvos

Grupė nagrinėjo keletą KYC duomenų surinkimo, jų saugojimo bei pateikimo FĮ būdų, siekdama optimizuoti KYC procesą: 1) kai duomenys surenkami ir saugomi centralizuotoje duomenų bazėje; 2) kai FĮ užklausia reikiamų duomenų vieno langelio principu per API ir juos išsaugo pas save (KYC API sistema).

#### a) Centralizuota duomenų bazė

Grupės nuomone, centralizuotoje duomenų bazėje turėtų būti surenkama ir saugoma visa FĮ reikalinga fizinių ir juridinių asmenų KYC informacija – valstybės registru ir kitų patikimų duomenų šaltinių duomenys, taip pat vartotojo suvedami duomenys. Modelio ekosistema veiktų *market place* principu, t. y. FĮ duomenų rinkėjai surenka duomenis ir parduoda, o FĮ pirkėjai – perka. Vartotojo duomenims suvesti gali būti kuriama atskira prieiga (geriausia – pasiekama internetu), sudarytos galimybės peržiūrėti, patvirtinti ar pakeisti duomenis apie save. Taip pat vartotojo pateiktus duomenis į centralizuotą duomenų bazę galėtų įkelti FĮ, kuriai duomenis pateikė vartotojas (FĮ veiktų kaip duomenų pardavėjas). Siekiant užtikrinti surenkamų duomenų kokybę, duomenų teikėjams turėtų būti nustatyti reikalavimai ir vykdoma jų priežiūra (pvz., duomenų teikėjais gali būti tik Lietuvos banko prižiūrimos FĮ, laikomasi tam tikrų standartų). KYC centralizuotos duomenų bazės kūrėjai turėtų palaikyti duomenų bazę ir užtikrinti duomenų saugumą, kitaip tariant, būtų duomenų valdytojais. Sprendime būtų galimos atskiros API sąsajos – per vieną sąsają tik gaunama informacija, o kita sąsaja atsisiunčiami visi duomenys apie klientą. Schemos dalyviai galėtų matyti, kokie duomenys ir iš kokių duomenų teikėjų pateikti. Duomenų teikėjai turėtų įsigyti kvalifikuotą elektroninį spaudą. Pagal antrąją Mokėjimo paslaugų direktyvą (PSD2), prie el. spaudo (*e. seal*) bus informacija apie paslaugų teikėjo veiklą.

#### b) KYC API sistema

KYC API sistema skiriasi nuo centralizuotos duomenų bazės pirmiausia tuo, kad nėra kuriama nauja duomenų bazė. Reikiamus duomenis FĮ iš valstybės registru ir kitų patikimų duomenų šaltinių galėtų paimti per specialią API sąsają formuojant vieną užklausą KYC API sprendimo valdytojui, o duomenis kiekviena FĮ saugotų individualiai (žr. 2 pav.). Esminis reikalavimas šiam sprendimui įgyvendinti yra vieno langelio principas – nesvarbu, kiek valstybės registru ar patikimų duomenų šaltinių egzistuoja Lietuvoje KYC duomenims surinkti, FĮ teiktų tik vieną užklausą schemos valdytojui ir gautų visus reikiamus duomenis, reikalingus KYC procesui. Schemos valdytojas būtų atsakingas už tinkamą integraciją su visais reikalingais valstybės registrais ir informacinėmis sistemomis, pats atnaujintų techninius sprendimus ir aprašymus, kai valstybės registru ar informacinių sistemų duomenys ar sąsajos būtų atnaujinti. Labai svarbu, kad, įgyvendinant vieno langelio principą, FĮ reikėtų pasirašyti sutartį dėl duomenų gavimo tik su tokios schemos valdytoju, o ne sudaryti sutartis su atskirais valstybės registrais ir informacinėmis sistemomis. Papildomai pažymima, kad kuriama KYC API sistema turėtų būti „bazinė paslauga“, kuri netrukdytų rinkoje



kurtis privačioms iniciatyvoms, siūlančioms FĮ ne tik pagrindinių KYC duomenų ištraukimą iš valstybės registru, bet ir papildomas paslaugas.

5 lentelė. Centralizuotos duomenų bazės ir sąsajomis pagrįsto KYC sprendimo galimybės ir grėsmės

Centralizuota duomenų bazė		Sąsajomis pagrįstas sprendimas	
Galimybės	Grėsmės	Galimybės	Grėsmės
<ul style="list-style-type: none"> <li>• <b>Didesnė duomenų aprėptis</b>, t. y. galimybė centralizuotai naudoti valstybės registru duomenis ir dalytis kliento pateikiamais duomenis.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Duomenų patikimumas</b> - sunku užtikrinti duomenų patikimumą, kai duomenis tiekia kitos FĮ.</li> <li>• <b>Nepasitikėjimas kitomis FĮ</b> – rizika, kad FĮ nepasitikės kitų FĮ surinktais duomenimis ir nesinaudos sprendimu.</li> <li>• <b>Griežtesnis teisinis, duomenų apsaugos reguliavimas</b>, nes duomenys laikomi pas trečiąją šalį, taip pat daugiau teisinio neapibrėžtumo (pvz., kaip įgyvendinti subjekto teisę būti pamirštam).</li> <li>• <b>Sudėtingesnis sistemos valdymas</b> – reikėtų gan dažnai sinchronizuoti duomenis su pirminėmis duomenų bazėmis, tai padidintų kaštus, papildomos investicijos į saugumo, kibernetinių atakų prevencijos užtikrinimą.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Didelis duomenų patikimumas</b>, nes naudojami tik valstybės registru duomenys.</li> <li>• <b>Užtikrinamas FĮ pasitikėjimas paslauga.</b></li> <li>• <b>Paprastesnis duomenų apsaugos reguliavimas</b>, nes duomenys nėra kaupiami centralizuotoje duomenų bazėje.</li> <li>• <b>Galimybė atpiginti valstybės duomenų paėmimo kaštus</b> – per sąsają būtų galimybė pasiimti iš valstybės registru tik reikiamus duomenis ir mokėti tik už juos.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Mažesnė duomenų aprėptis</b> – tik valstybės registru duomenys.</li> </ul>
<p><b>Svarbu.</b> Dar nesukurta paslauga, kuri leistų FĮ iš valstybės registru ir informacinių sistemų pasiimti ne visą duomenų masyvą, o tik reikalingus duomenis. Kadangi mokama už kiekvieną „pasiimtą“ duomenį, FĮ tai brangiai kainuoja. Naujas optimizuotas KYC sprendimas pirmiausia leistų FĮ pasiimti iš valstybės registru ir informacinių sistemų tik jiems reikalingus duomenis, todėl sumažėtų FĮ kaštai ir būtų geriau užtikrintas deramas asmens duomenų tvarkymas, atsisakant perteklinio duomenų tvarkymo ir duomenų dubliavimo (įskaitant perteklinių ar besikartojančių asmens duomenų, sudarančių duomenų masyvą, perdavimą FĮ).</p>			

**Grupės pozicija.** Grupė, įvertinusi alternatyvių KYC procesų optimizavimo naudas ir grėsmes, sutarė tolesnėje analizėje koncentruotis į KYC API sprendimą, o centralizuotos duomenų bazės sprendimo toliau nenagrinėti. Grupė atkreipia dėmesį į tai, kad, įgyvendinant vieno langelio principą KYC API sprendime, FĮ turi būti sudarytos sąlygos sudaryti sutartį tik su sprendimo valdytoju. Grupė pažymi, kad KYC API sistema turėtų būti „bazinė paslauga“, kuri netrukdytų rinkoje kurtis privačioms iniciatyvoms, siūlančioms FĮ ne tik pagrindinių KYC duomenų ištraukimą iš valstybės registru, bet ir papildomas paslaugas.

Be to, pažymima, kad, įgyvendinus KYC API sprendimą, verta svarstyti galimybę dalį individualių KYC anketinių duomenų, kurie nesaugomi jokiuose patikimuose duomenų šaltiniuose, saugoti atskiroje duomenų bazėje, pvz., kurią valdytų KYC API sprendimo valdytojas, o ją pildytų patys FĮ klientai pagal poreikį (t. y. praplėsti KYC API sprendimą). Tokie duomenys galėtų būti: telefono numeris, elektroninio pašto adresas, pajamų šaltinis, lėšų, turto kilmė, įmonės struktūrinė schema, galutiniai naudos gavėjai (kai galutiniai naudos gavėjai yra užsienio subjektai) ir kita tam tikros finansų srities informacija, kuri šiuo metu nesaugoma patikimuose duomenų šaltiniuose (pvz., informacija, susijusi su finansinėmis draudimo paslaugomis).

## 5.2. Tarptautinis kontekstas, suderinamumas su kitomis duomenų bazėmis ir (arba) užsienio sprendimais

Kai kuriose pasaulio valstybėse kuriama centralizuota duomenų bazė arba kuriamas KYC optimizavimo sprendimas naudojant sąsajas. Automatizuotas KYC procesas veikia Jungtinėje Karalystėje, Švedijoje, Norvegijoje, kur FĮ ir kitiems rinkos dalyviams suteikiama prieiga prie oficialių registru.

2015 m. Jungtinėje Karalystėje buvo įsteigta „Payments Strategy Forum“ institucija, panaši į lietuvišką Mokėjimų tarybą. Viena iš prioritetinių institucijos sričių – KYC proceso optimizavimas. „Payments Strategy Forum“ sukūrė KYC optimizavimo sprendimą „Trusted KYC Data Sharing“<sup>4</sup>. Šis modelis paremtas KYC duomenų dalijimosi tarp FĮ principu.

Singapūre kuriama e-KYC platforma, kurios valdytojas – valstybės įstaiga „Monetary Authority of Singapore“ (MAS). e-KYC bandomasis projektas pradėtas vykdyti 2017 m. su dviem Singapūro bankais, bet apėmė tik juridinių asmenų duomenis. Sprendimas paremtas „MyInfo“<sup>5</sup> – asmens duomenų platforma, kurioje yra vyriausybės patvirtinti asmens duomenys (pavyzdžiui, nacionalinis asmens kodas, gyvenamosios vietos adresas). „MyInfo“ sukūrė Finansų ministerija ir „GovTech“, skaitmeninimo ir duomenų strategijos agentūra Singapūre. Projektas sustojo dėl lėšų stokos, bet planuojama, kad bus atnaujintas išanalizavus padarytas klaidas.

Siekdamos optimizuoti fizinių asmenų KYC procesus, Singapūro institucijos bando plėsti „MyInfo“ registro renkamų duomenų sąrašą ir turi viziją per įsteigtą duomenų valdytoją teikti KYC duomenis FĮ vieno langelio principu. Pažymėtina, kad toks vieno langelio principas jau įgyvendintas, nes FĮ identifikacijos duomenis ir dalį KYC duomenų apie fizinius asmenis gali gauti iš „MyInfo“ registro automatizuotu būdu per programinę sąsają. Fiziniai asmenys, prisijungę prie „MyInfo“, gali duoti ar atšaukti sutikimą dalytis jų duomenimis, matyti, kokioms įstaigoms jų duomenys buvo pateikti.

Skandinavijoje penki dideli bankai imasi savarankiškos iniciatyvos kurti KYC dalijimosi duomenimis infrastruktūrą ir paskelbė apie projektą „Nordic KYC utility“<sup>6</sup>. Projektas apimtų didžiuosius 5 bankus, vėliau prie jo galėtų jungtis ir kitos FĮ. Pradiniu etapu projektas orientuotas į juridinių asmenų, vėliau – ir fizinių asmenų KYC proceso optimizavimą. Duomenų apsikeitimo būdas tarp FĮ kol kas išsamiau nedetalizuojamas.

Estijoje ir Latvijoje aktyviai kalbama apie KYC optimizavimą, tačiau konkrečių sprendimų dar nėra priimta. Svarbu pažymėti, kad Estijoje ir Latvijoje KYC procesas klientams jau dabar nėra sudėtingas, nes FĮ neprivalo surinkti anketinių duomenų iš savo klientų ir vėliau juos sutikrinti su patikimais duomenų šaltiniais, todėl šioje srityje Latvija ir Estija, Grupės nuomone, turi pažangesnį sprendimą.

Grupė nagrinėjo ir EK iniciatyvas dėl KYC ir bendro santykių su klientu pradėjimo (*on-boarding*). EK įkūrė Ekspertų darbo grupę dėl el. atpažinties ir nuotolinių KYC procesų (toliau – EK grupė). EK grupė turės pateikti tarptautiniu lygmeniu veikiančio nuotolinio KYC proceso sprendimo pasiūlymą. EK grupė susiskirsčiusi į dvi dalis – teisinę ir praktinę. Praktinė EK grupės dalis, nagrinėjanti atributus, yra labiau pažengusi. Atributų analizė buvo vykdyta eIDAS reglamento<sup>7</sup>

<sup>4</sup> <<https://implementation.paymentsforum.uk/key-documents>>

<sup>5</sup> <<https://www.singpass.gov.sg/myinfo/common/aboutus>>

<sup>6</sup> <<https://www.pymnts.com/news/international/2018/nordic-banks-collaborate-aml-kyc/>>

<sup>7</sup> 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB.



kontekste. Kol kas EK grupė bando sudėlioti pirmą pasiūlymą dėl *Minimum Viable KYC attribute framework*, didelis dėmesys skiriamas klausimams, kokie atributai reikalingi, koks turėtų būti jų patikimumo lygmuo. EK grupė orientuojasi į vieną tarptautinį standartą, o ne nacionalinius ir (arba) regioninius sprendimus. EK grupė atributo patikimumą sieja su tuo, kaip atributas gautas (pavyzdžiui, *trusted source*, *recognized independent third party* ar pats klientas pateikė atributą) ir kaip jis patikrintas (ar gavimo metu nepažeistas integralumas). Kai pats klientas pateikia atributą, tai laikoma žemiausiu patikimumu. EK grupė nagrinėja standartinį KYC procesą, supaprastinto ar sustiprinto proceso nenagrinės. Nors per pirmuosius susitikimus buvo manoma, kad tarptautiniam KYC sprendimui gali būti pritaikytas tik eIDAS, dabar vis labiau linkstama prie vaizdo *on boarding*.

**Grupės pozicija.** Grupės formuluojamas optimizuoto KYC proceso pasiūlymas panašiausias į jau dalinai įgyvendintą Singapūro sprendimą. Pažymėtina, kad KYC procese galima naudoti ne tik valstybės registrų ir informacinių sistemų, bet ir mažiau patikimus duomenis, todėl Grupė rekomenduoja, kuriant KYC API sprendimą Lietuvoje, peržiūrėti EK grupės naujausius priimtus sprendimus ir įvertinti galimybę saugoti kitus, ne valstybės registrų ir informacinių sistemų duomenis, jiems sukuriant atskirą registrą, kurį valdytų KYC API sprendimo valdytojas. Mažesnio patikimumo lygmens duomenys reikalingi tarptautiniam KYC sprendimui ir tada, kai valstybės registrų ir informacinių sistemų duomenys per brangūs arba neprieinami.

KYC API sprendimo būdas ateityje galėtų būti nesudėtingai suderinamas su kitais užsienyje sukurtais panašiais sprendimais, Grupė neišvengia techninių ar teisinių apribojimų tai realizuoti. Užklausa apie Lietuvos duomenų subjektą per sąsają galėtų pateikti ir užsienio FĮ, jei tam būtų teisinis pagrindas. Techninis sprendimas turi būti sudarytas taip, kad užklausa teikėjai (FĮ) nebūtų apribojami pagal įsisteigimo šalį. Jei užsienio FĮ pasirašytų duomenų gavimo sutartį su schemos valdytoju ir integruotų Lietuvos duomenų valdytojo techninius sprendimus, tokia FĮ galėtų tapti schemos dalyviu.

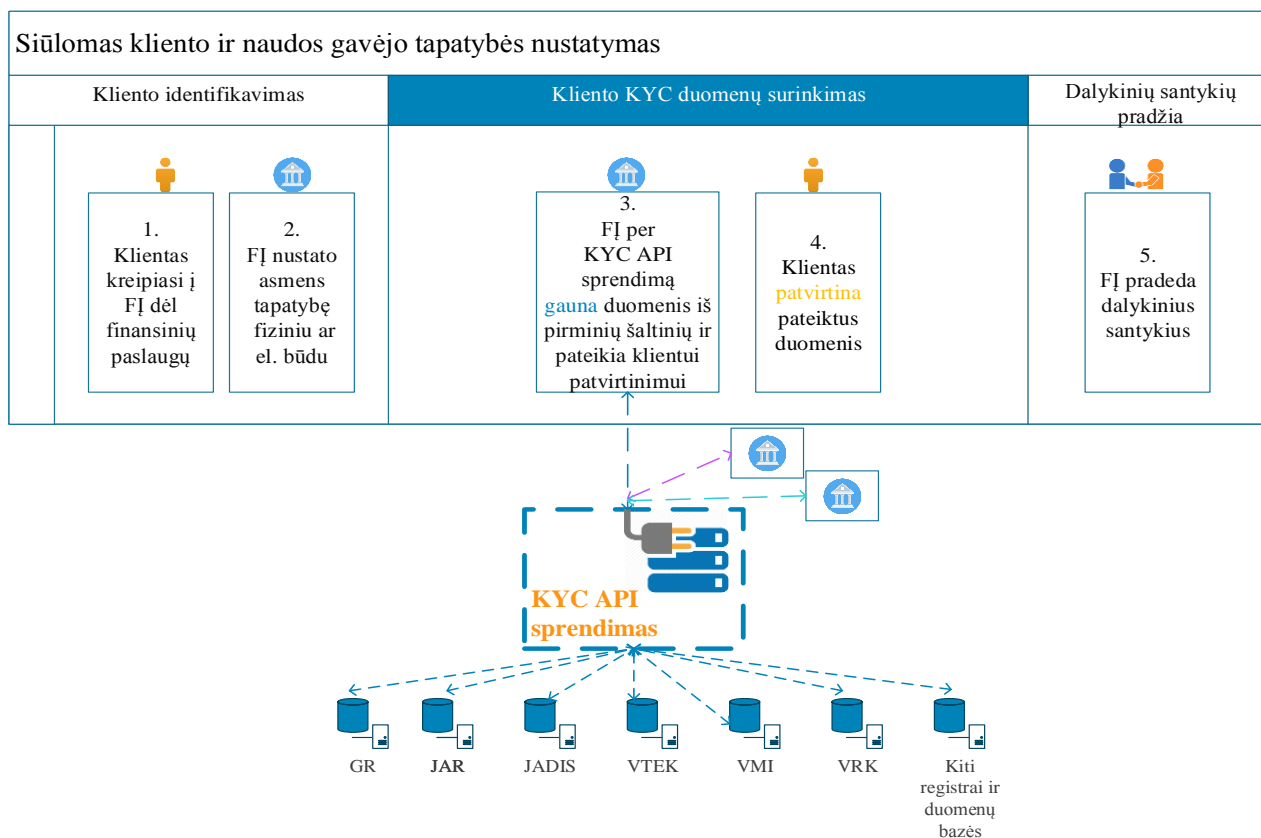
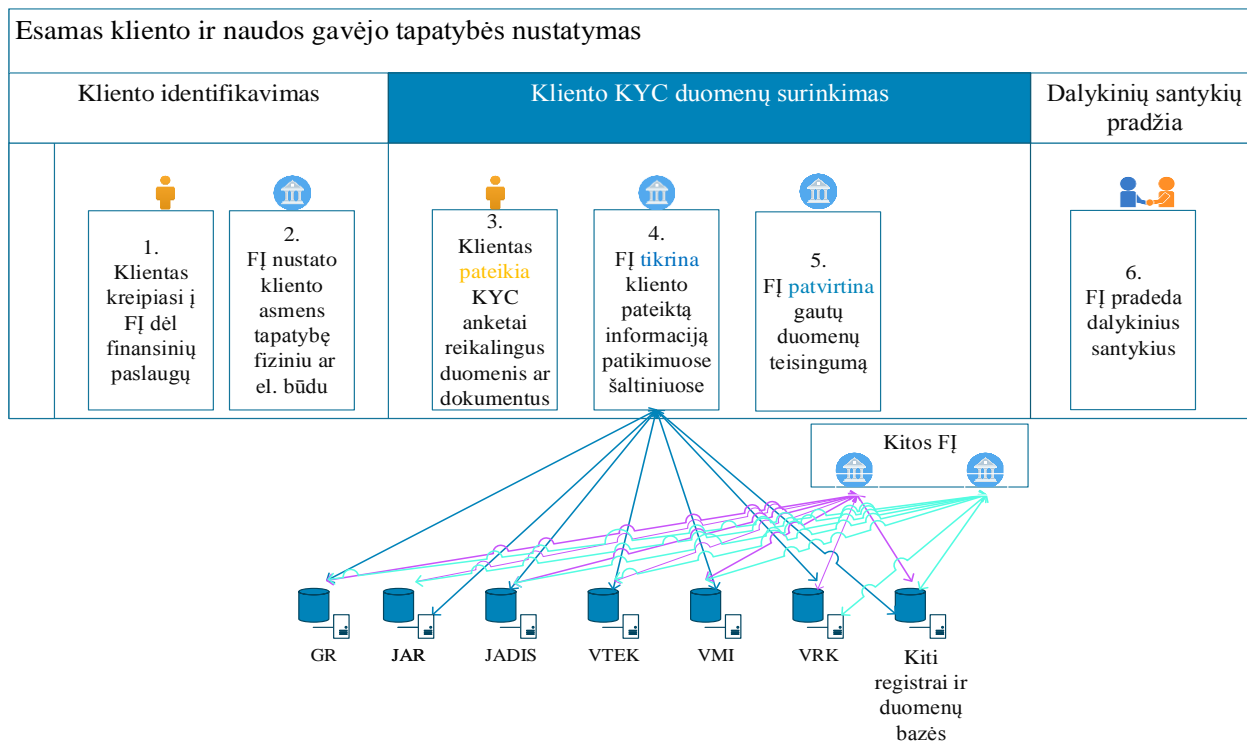
Taip pat svarbu, kad sąsajos techninis sprendimas IT požiūriu būtų suprojektuotas ir suprogramuotas taip, kad užklausa galėtų būti pateikiama užsienio analogiškos sąsajos arba „centralizuoto“ KYC sprendimo valdytojui, t. y. numatyti, kad užklausa galėtų būti siunčiama ne tik Lietuvos, bet ir užsienio valstybių registrams ar užsienio analogiškų KYC schemų valdytojams.

## 6. Siūlomas optimizuoto KYC proceso modelis

Siekdama pagerinti kliento patirtį KYC procese, optimizuoti duomenų surinkimo kaštus, atsisakyti duomenų dubliavimo ir perteklinių procesų, Grupė siūlo KYC optimizuoti Lietuvoje sukurti KYC API sprendimą, kuris veiktų taip:

- A. FĮ **identifikuoja** klientą pagal dabartinius PPTFPĮ reikalavimus (identifikavimo žingsnio Grupė nenagrinėja)
- B. FĮ, sėkmingai identifikavusi klientą, inicijuoja automatinį duomenų gavimą iš patikimų ir nepriklausomų duomenų šaltinių (valstybės registrų ir informacinių sistemų) per standartizuotą KYC API sąsają sprendimą;
- C. klientas pateikia trūkstamą informaciją;
- D. klientas patvirtina automatinio būdu užpildytą (angl. *prefill*) ir savo pateiktą informaciją.

2 pav. Esamo KYC proceso ir siūlomo optimizuoto KYC proceso schema



Daugumą pagal PPTFPĮ 10 straipsnio 1 ir 2 dalis reikalaujamų duomenų savo valdomuose registruose ir informacinėse sistemose tvarko ir saugo RC: GR, JAR, JADIS, Adresų registre, ĮR, NRVAR, Vedybų sutarčių ir kituose registruose, taip pat tobulina JADIS, Politinių partijų narių sąrašų informacinę sistemą, Piniginių lėšų apribojimų informacinę sistemą (žr. 1 priedą „KYC duomenų šaltiniai“).

**Grupės pozicija.** Grupė siūlo kurti nacionalinį KYC API sprendimą dėl universalių duomenų gavimo iš viešųjų registrų ir informacinių sistemų, nekuriant naujos duomenų bazės. Sprendimo valdytojas (valstybinis, privatus ar kt.) bazinę paslaugą dėl universalių duomenų turėtų teikti vienodomis sąlygomis visoms FĮ. Papildomas su KYC procesu susijusias paslaugas galėtų kurti ir siūlyti kiti paslaugų teikėjai.

KYC API sprendimą siūloma kurti naudojantis RC duomenimis, o naujai sukurtus registrus (pavyzdžiui, VTEK – dėl PEP arba RC – galutinių naudos gavėjų registrą) integruoti į tą patį sprendimą vėlesniuose etapuose.

## 7. KYC API sprendimo valdytojas

KYC API sprendimo valdytoju ir paslaugos teikėju, kuris pagal reguliavimo pokyčius ir FĮ poreikius koreguotų pateikiamus duomenis ir tobulintų technologinius sprendimus, gali būti įvairios institucijos ar privatūs subjektai (žr. 6 lentelę).

6 lentelė. Galimų KYC API sprendimo valdytojų pliusai ir minusai

	PLIUSAI	MINUSAI
<b>Valstybės institucijos</b> <i>Singapūro atvejis</i>	<ul style="list-style-type: none"> <li>Tikėtina, kad reikiami teisėkūros procesai vyktų sklandžiau (t. y. jei reikėtų kokio teisės akto pakeitimo, tai būtų atlikta greičiau).</li> <li>Tikėtina, kad būtų išspręstas FĮ atsakomybės klausimas tais atvejais, kai valstybės registras, pavyzdžiui, duotų atsakymą, kad asmuo nėra PEP, bet paaiškėtų, kad yra.</li> </ul>	<ul style="list-style-type: none"> <li>Sudėtingas įgyvendinimas (ne viešojo administravimo funkcija, reikia pateisinti valstybės dalyvavimą tokio sprendimo veikloje ir rasti instituciją, kuriai priklausytų priimti šį sprendimą).</li> <li>Neprognuojama kainodara.</li> <li>Nelankstumas inovacijoms.</li> <li>Neprognuojamas veiklos tęstinumas (pasikeitus pozicijai (valdžiai) KYC API sprendimo veikla galėtų būti bet kada nutraukta).</li> <li>Rizika riboti konkurenciją.</li> </ul>
<b>Privati įstaiga, sukurta iš kelių FĮ dalininkų</b> <i>Skandinavų atvejis</i>	<ul style="list-style-type: none"> <li>Kontroliuojama kainodara (jei tikslas – ne pelnas iš veiklos, o investicijų padengimas ir sistemos palaikymas).</li> <li>Lankstumas inovacijoms.</li> <li>Tikėtina, kad dėl bendro intereso būtų išspręstas veiklos tęstinumo klausimas (t. y. iškilus grėsmei dėl veiklos nutraukimo būtų ieškoma veiklos tęsimo būdų ir sprendimų).</li> </ul>	<ul style="list-style-type: none"> <li>Valdymo modelio sudėtingumas (kiek FĮ dalyvauja steigime, kokiomis proporcijomis, teisių perleidimas, naujų dalyvių priėmimas ir kt.).</li> <li>Galimi priekaištai dėl neskaidrios kainodaros (jei bus skirtumų tarp „saviems“, t. y. steigėjams, ir „kitiems“).</li> <li>Duomenų surinkimo procesas, surinktų duomenų patikimumas, atsiribojimas nuo atsakomybės.</li> </ul>
<b>Technologinė (teisinė) atitikties įmonė</b> <i>IBM ir SWIFT atvejis</i>	<ul style="list-style-type: none"> <li>Nesudėtingas įsteigimas.</li> <li>Greitas sprendimų priėmimas.</li> <li>Lankstumas inovacijoms.</li> </ul>	<ul style="list-style-type: none"> <li>Nekontroliuojama kainodara (dėl pelno siekimo).</li> <li>Veiklos tęstinumo garantijos nebuvimas (verslo tvarumo klausimas).</li> <li>Duomenų surinkimo procesas, surinktų duomenų patikimumas, atsiribojimas nuo atsakomybės.</li> </ul>

5 iš 7 pagrindinių grupės narių, atstovaujančių skirtingoms institucijoms ir asociacijoms, apklausoje balsavo dėl galimo KYC API sprendimo valdytojo. Du valstybės institucijų (Lietuvos banko ir Finansų ministerijos) atstovai susilaikė nuo balsavimo, kiti 3 pagrindiniai nariai (atstovaujantys asociacijai „Fintech Lietuva“, Mykolo Romerio universitetui, Mokėjimo ir elektroninių pinigų įstaigų asociacijai) mano, kad KYC API sprendimo valdytoju turėtų būti valstybės įstaiga.

Pažymėtina, kad ir kiti grupės nariai išreiškė savo poziciją – 6 nepagrindiniai grupės nariai (atstovaujantys Lietuvos bankų asociacijai, asociacijai „Fintech Lietuva“, asociacijai „Fintech Hub LT“, Mokėjimo ir elektroninių pinigų įstaigų asociacijai) siūlo KYC API sprendimo valdytoju valstybės įstaigą, vienas narys (atstovaujantis Mokėjimo ir elektroninių pinigų įstaigų asociacijai) – KYC API sprendimo valdytoju privačią įstaigą, sukurtą iš kelių FĮ, ir vienas narys (atstovaujantis „Fintech Lietuva“) – technologinę (teisinę) atitikties įmonę.

7 lentelė. Valstybės institucijų, kaip galimų KYC valdytojų, plusai ir minusai

<b>Galimas KYC sprendimo valdytojas</b>	<b>PLUSAI</b>	<b>MINUSAI</b>
<b>IVPK</b>	<ul style="list-style-type: none"> <li>• Būti vienu langeliu teikiant išrinktus duomenis viešajam sektoriui yra vienas iš pagrindinių įstaigos tikslų.</li> </ul>	<ul style="list-style-type: none"> <li>• Neprognozuojamas veiklos tęstinumas (pasikeitus pozicijai ir (arba) valdžiai, KYC valdytojo veikla galėtų būti bet kada nutraukta).</li> <li>• Reikalingi teisiniai pakeitimai norint teikti duomenis FĮ.</li> <li>• Neaišku, ar tiks jau sukurta (esama) vieno langelio techninė realizacija, reikia techninių prisijungimų prie dalies registrų.</li> <li>• Daugumą duomenų IVPK imtų iš RC.</li> </ul>
<b>RC</b>	<ul style="list-style-type: none"> <li>• Tvarko daugiausiai KYC reikalingų duomenų registrų.</li> <li>• Turi technologinių priemonių aplikacijai sukurti, nes darė panašių projektų.</li> <li>• Gali išrinkti tik tuos duomenis, kurių reikia, o ne visą paketą, dėl ko, tikėtina, būtų patrauklesnė kainodara.</li> <li>• Pagrindinė RC veikla yra registrų objektų registravimas ir patikimos informacijos, duomenų teikimas visiems piliečiams, rinkos dalyviams ir valdžios bei valdymo institucijoms.</li> </ul>	<ul style="list-style-type: none"> <li>• Didelis biurokratinis aparatas.</li> <li>• Galimos pertvarkos, neaišku, kaip greitai gali imtis naujų projektų.</li> </ul>
<b>Nauja įstaiga po EIMIN (pvz., VŠĮ)</b>	<ul style="list-style-type: none"> <li>• Greitas sprendimų priėmimas, yra lėšų.</li> <li>• Kontroliuojama kainodara (jei tikslas – ne pelnas iš veiklos, o investicijų padengimas ir sistemos palaikymas).</li> <li>• Aiški valdymo struktūra ir atsakomybės.</li> <li>• Būtų siekiama vieno tikslo – KYC optimizavimo (vėliau galima būtų prijungti ir AML funkcijas).</li> </ul>	<ul style="list-style-type: none"> <li>• Gali būti sunku pagrįsti naujos įstaigos steigimo būtinumą.</li> <li>• Nebūtų sinergijos dėl esamos infrastruktūros, darbuotojų pasitelkimo.</li> <li>• Galimai didesni pradiniai kaštai.</li> </ul>

5 iš 7 pagrindinių grupės narių, atstovaujančių skirtingoms institucijoms ir asociacijoms, apklausoje balsavo dėl galimo KYC API sprendimo valdytojo. Du valstybės institucijų (Lietuvos banko ir Finansų ministerijos) atstovai susilaikė nuo balsavimo, kiti 3 pagrindiniai nariai (atstovaujantys „Fintech Lietuva“, Mykolo Romerio universitetui, Mokėjimo ir elektroninių pinigų įstaigų asociacijai) mano, kad KYC API sprendimo valdytoju turėtų būti RC.

Pažymėtina, kad ir kiti grupės nariai išreiškė savo poziciją dėl valstybės įstaigos, kuri galėtų valdyti KYC API sprendimą – 4 nepagrindiniai grupės nariai (atstovaujantys Lietuvos bankų asociacijai, asociacijai „Fintech Lietuva“, asociacijai „Fintech Hub LT“) siūlo KYC API sprendimo valdytoju RC, 2 nariai (atstovaujantys Mokėjimo ir elektroninių pinigų įstaigų asociacijai) – KYC API sprendimo valdytoju sukurtą naują įstaigą po EIMIN.

**Grupės rekomendacija.** Galimo KYC API sprendimo valdytoju galėtų būti valstybės institucija. Daugumos grupės narių nuomone, tinkamiausias valdytojas būtų RC, nes RC jau šiuo metu tvarko beveik visus valstybės registrus ir informacines sistemas, kurie šiuo metu veikia ir yra naudojami KYC procese. Pirminiame etape kuriant KYC API sprendimą RC reikėtų mažiausiai teisinių pakeitimų. Kuriant naujus valstybės registrus, kurių duomenys naudojami KYC procese, svarbu įvertinti galimybes juos įtraukti į KYC API sprendimą.

## 8. Teisinės KYC proceso optimizavimo kliūtys ir rekomendacijos

Šiuo metu galiojančios redakcijos PPTFPĮ apriboja FĮ galimybę tobulinti kliento bei galutinio naudos gavėjo tapatybės nustatymo procesus (tiek dalykinių santykių užmezgimo metu, tiek ir duomenų atnaujinimo metu), efektyviai panaudoti duomenis (dokumentus), gautus iš patikimų ir nepriklausomų šaltinių (pavyzdžiui, iš valstybės registrų ar informacinių sistemų), taip pat išvengti duomenų (dokumentų) dubliavimo. PPTFPĮ yra įtvirtintas principas, kad kliento ir galutinio naudos gavėjo tapatybei nustatyti reikiamus duomenis (dokumentus) pirmiausia reikia gauti iš kliento, o paskui juos patikrinti patikimuose ir nepriklausomuose šaltiniuose (PPTFPĮ 9 straipsnio 13 ir 15 dalys, 10 straipsnio 2 ir 3 dalys). Minėtos PPTFPĮ nuostatos reiškia, kad klientas pats FĮ privalo pateikti visus reikiamus duomenis (dokumentus), nors tam tikri duomenys (dokumentai) gali būti prieinami FĮ patikimuose ir nepriklausomuose šaltiniuose tiesiogiai. Toks PPTFPĮ įtvirtintas kliento ir galutinio naudos gavėjo tapatybės nustatymo procesas nėra įtvirtintas nei 2015 m. gegužės 20 d. Europos Parlamento ir Tarybos direktyvoje (ES) 2015/849, nei 2018 m. gegužės 30 d. Europos Parlamento ir Tarybos direktyvoje (ES) 2018/843, todėl, Grupės nuomone, yra perteklinis. Be to, Grupės žiniomis, tiek Latvijoje, tiek Estijoje kliento ir galutinio naudos gavėjo tapatybei nustatyti reikalingų duomenų (dokumentų) gavimas tiesiogiai iš patikimų ir nepriklausomų šaltinių (registrų), nereikalaujant jų iš kliento, yra galimas.

Dėl pirmiau nurodytų PPTFPĮ reikalavimų kliento ir galutinio naudos gavėjo tapatybės nustatymo procesas yra neefektyvus ir nepatogus klientui, o duomenys (dokumentai) yra dubliuojami. Pavyzdžiui, vadovaudamasis PPTFPĮ 10 straipsnio 2 dalies reikalavimu, klientas FĮ pateikia registracijos išrašą iš JAR, jo nuorašą arba elektroninį sertifikuotą išrašą, o paskui FĮ patikrina kliento pateiktą dokumentą tame pačiame JAR (ir gali gauti netgi naujesnę informaciją, nei pateikia klientas).

Šiuo metu Seime svarstomas PPTFPĮ 2, 7, 9, 10, 19, 20, 49 straipsnių, priedų pakeitimo ir įstatymo papildymo 251 ir 252 straipsniais įstatymo projektas (toliau – Įstatymo projektas). Įstatymo projekte numatyti pakeitimai susiję su galimybe kliento ir galutinio naudos gavėjo tapatybei nustatyti

reikalingus dokumentus, duomenis ar informaciją tiesiogiai gauti iš valstybės informacinių sistemų ar registru, neprašant jų iš klientų. Grupė pozityviai vertina numatomus pokyčius, tačiau, įvertinusi Įstatymo projekto 4 straipsnį, Grupė išvelgia, kad reikia papildomų pokyčių (žr. Grupės rekomendaciją (Nr. 1)).

Šiuo metu tiesioginis duomenų (dokumentų) gavimas iš patikimų ir nepriklausomų šaltinių laikytinas tinkamu kliento bei galutinio naudos gavėjo duomenų atnaujinimui dalykinių santykių metu. Tokią poziciją yra nurodęs ir Lietuvos bankas 2018 m. liepos 24 d. viešai paskelbtame finansų rinkos dalyviams skirtame atsakyme. Tačiau minėtame atsakyme nurodyta, kad atnaujinti duomenys visais atvejais turi būti pateikiami klientui jų teisingumui patvirtinti ir (ar) jiems koreguoti, papildyti. Grupės nuomone, toks reikalavimas nėra būtinas, nes yra atvejų, kai periodinio duomenų atnaujinimo metu FĮ nenustato jokių požymių, kad anksčiau kliento pateikti ir patvirtinti duomenys pakito, t. y. kliento anksčiau FĮ pateikti duomenys atitinka tuos, kurie yra gaunami iš patikimų ir nepriklausomų šaltinių, kliento veikla ir jo įprastas bendradarbiavimas su FĮ nėra pakitę, nėra paaiškėję kitų reikšmingų aplinkybių.

**Grupės rekomendacija (Nr. 1).** Atsižvelgdama į pirmiau išdėstytus argumentus, Grupė siūlo Finansinių nusikaltimų tyrimo tarnybai prie Vidaus reikalų ministerijos koreguoti PPTFPĮ ir sudaryti galimybę FĮ naudoti duomenis (dokumentus), gautus tiesiogiai iš patikimų ir nepriklausomų šaltinių, dalykinių santykių užmezgimo metu. Svarbu pabrėžti, kad visais atvejais, prieš naudodama duomenis (dokumentus), gautus tiesiogiai iš patikimų ir nepriklausomų šaltinių, FĮ identifikuotą klientą (fizinį asmenį) arba kliento (fizinio ar juridinio asmens) atstovą (fizinį asmenį), remdamasi asmens tapatybę patvirtinančiu dokumentu asmeniui dalyvaujant fiziškai ar kitais PPTFPĮ 11 straipsnyje numatytais nuotolinio identifikavimo būdais. Identifikavus klientą (fizinį asmenį) arba kliento (fizinio ar juridinio asmens) atstovą (fizinį asmenį), FĮ tolesnius duomenis (dokumentus), reikalingus kliento ir galutinio naudos gavėjo tapatybei nustatyti (pavyzdžiui, duomenis apie juridinio asmens vadovus, dalyvius, galutinius naudos gavėjus), tiesiogiai gautų iš patikimų ir nepriklausomų šaltinių ir pateiktų klientui ar jo atstovui patvirtinti duomenų teisingumą ir (ar) juos koreguoti, papildyti. Tiesioginis duomenų (dokumentų) gavimas iš patikimų ir nepriklausomų šaltinių sudarytų sąlygas efektyviau, paprasčiau ir klientams patogesniu būdu naudotis FĮ teikiamomis paslaugomis, būtų išvengiama duomenų (dokumentų) dubliavimo.

Grupė siūlo tokius Įstatymo projekto pakeitimus:

**„4 straipsnis. 10 straipsnio pakeitimas**

1. Papildyti 10 straipsnį nauja 4 dalimi:

„4. Finansų įstaigos ir kiti įpareigotieji subjektai turi teisę gauti šiame įstatyme nurodytus kliento ar naudos gavėjo tapatybei nustatyti reikalingus dokumentus, duomenis ar informaciją tiesiogiai iš valstybės informacinių sistemų ar registru ir nereikalauti iš kliento pačiam pateikti minėtus dokumentus, duomenis ar informaciją, jeigu klientas finansų įstaigos ar kito įpareigotojo subjekto dokumentus, duomenis ar informaciją, gautus tiesiogiai iš valstybės informacinių sistemų ar registru, patvirtina (~~pažangiuoju elektroniniu ar kvalifikuotuoju elektroniniu~~) parašu. **Finansų įstaigos ir kiti įpareigotieji subjektai turi teisę nereikalauti, kad klientas finansų įstaigos ar kito įpareigotojo subjekto tiesiogiai iš valstybės informacinių sistemų ar registru gautus dokumentus, duomenis ar informaciją patvirtintų parašu, jeigu tokie dokumentai, duomenys ar informacija nesiskiria nuo anksčiau kliento parašu patvirtintų dokumentų, duomenų ar informacijos, taip pat jeigu tokie dokumentai, duomenys ar informacija yra gauti iš Gyventojų registro.**“



2. Buvusias 10 straipsnio 4–6 dalis laikyti atitinkamai 5–7 dalimis.“

**KOMENTRAS:**

*Atkreiptinas dėmesys į tai, kad PPTFPĮ 12 straipsnyje ir taip jau yra numatyta pareiga klientui patvirtinti parašu ir antspaudu (jeigu jis antspaudą privalo turėti pagal jo veiklą reguliuojančius teisės aktus) duomenų apie naudos gavėjo tapatybę teisingumą, todėl FĮ bei kiti įpareigotieji subjektai visais atvejais **užtikrintų naudos gavėjo tapatybės duomenų patvirtinimą parašu**. Taip pat reikalavimo – patvirtinimą gauti klientui pasirašant pažangiuoju ar kvalifikuotu parašu – įkėlimas į straipsnį, kuriame reglamentuojamas kliento tapatybės nustatymo procesas klientui fiziškai dalyvaujant, apskritai nėra teisingas ir ribotą FĮ galimybę naudotis šia įstatymo nuostata klientui dalyvaujant fiziškai, t. y. atvykus į FĮ padalinį.*

*Taip pat, Grupės nuomone, siekiant teisinio aiškumo ir apibrėžtumo, analogišku tekstu (kaip kad siūloma papildyti 10 straipsnį nauja 4 dalimi) turi būti papildyta ir 11 straipsnio 3 dalis, todėl siūloma:*

**Pakeisti 11 straipsnio 3 dalį ir ją išdėstyti taip:**

3. Nustatydami kliento ir naudos gavėjo tapatybę klientui fiziškai nedalyvaujant, finansų įstaigos ir kiti įpareigotieji subjektai privalo imtis šio įstatymo 9 straipsnyje nustatytų priemonių ir nustatyti bei patikrinti ir kliento, ir naudos gavėjo tapatybę, gauti šio įstatymo 10 ir 12 straipsniuose nurodytus duomenis, kliento ir naudos gavėjo tapatybei nustatyti panaudoti papildomus duomenis, dokumentus ar papildomą informaciją, kuri leistų įsitikinti kliento tapatybės autentiškumu, patikrinti, ar yra aplinkybių taikyti sustiprintą kliento tapatybės nustatymą. **Finansų įstaigos ir kiti įpareigotieji subjektai turi teisę gauti šiame įstatyme nurodytus kliento ar naudos gavėjo tapatybei nustatyti reikalingus dokumentus, duomenis ar informaciją tiesiogiai iš valstybės informacinių sistemų ar registų ir nereikalauti iš kliento pačiam pateikti minėtus dokumentus, duomenis ar informaciją, jeigu klientas finansų įstaigos ar kito įpareigotojo subjekto dokumentus, duomenis ar informaciją, gautus tiesiogiai iš valstybės informacinių sistemų ar registų, patvirtina parašu. Finansų įstaigos ir kiti įpareigotieji subjektai turi teisę nereikalauti, kad klientas finansų įstaigos ar kito įpareigotojo subjekto tiesiogiai iš valstybės informacinių sistemų ar registų gautus dokumentus, duomenis ar informaciją patvirtintų parašu, jeigu tokie dokumentai, duomenys ar informacija nesiskiria nuo anksčiau kliento parašu patvirtintų dokumentų, duomenų ar informacijos, taip pat jeigu tokie dokumentai, duomenys ar informacija yra gauti iš Gyventojų registro.“**

Grupė taip pat siūlo apsvarstyti kitą alternatyvą – nekeisti įstatymo 10 ir 11 straipsnių, kurie yra skirti atskiriems tapatybėms nustatymo būdams (klientui dalyvaujant fiziškai ir klientui nedalyvaujant fiziškai), o siūloma nuostata papildyti tik įstatymo 9 straipsnį, kuris yra skirtas bendriesiems kliento ir naudos gavėjo tapatybės nustatymo reikalavimams, taikomiems visiems tapatybės nustatymo būdams (tiek klientui dalyvaujant fiziškai, tiek nedalyvaujant), nustatyti.

**Grupės rekomendacija (Nr. 2).** Atsižvelgdama į pirmiau išdėstytus argumentus, Grupė siūlo Lietuvos banko priežiūros tarnybai, kol Įstatyme bus numatyta tokia galimybė, kliento ir naudos gavėjo duomenų atnaujinimo metu leisti FĮ savo nuožiūra, remiantis rizika pagrįstu vertinimu, nusistatyti atvejus, kai:

a) duomenų teisingumui patvirtinti ir(arba) jiems koreguoti ir papildyti būtina kreiptis į klientą. Pavyzdžiui, tokiu atveju, kai patikimuose ir nepriklausomuose šaltiniuose nustatytas dalyvių pasikeitimas, o klientas apie tokį pasikeitimą nebuvo informavęs FĮ;

b) duomenys gali būti atnaujinami nesikreipiant į klientą. Pavyzdžiui, kai periodinio duomenų atnaujinimo metu nenustatoma jokių pokyčių tarp kliento anksčiau FĮ pateiktų duomenų bei duomenų atnaujinimo metu patikimuose ir nepriklausomuose šaltiniuose esančių duomenų.

Leidus FĮ savo nuožiūra nustatyti minėtus atvejus, būtų išvengiama atvejų, kai periodinio duomenų atnaujinimo metu į klientą kreipiamasi prašant patvirtinti tuos pačius, t. y. kliento anksčiau FĮ pateiktus ir nepasikeitusius duomenis, pavyzdžiui, duomenis apie juridinio asmens vadovus, dalyvius, galutinius naudos gavėjus. Toks duomenų atnaujinimo procesas, Grupės nuomone, būtų efektyvesnis, paprastesnis ir patogesnis klientams. Atitinkamai yra pateiktas pasiūlymas koreguoti Įstatymo projektą (žr. Grupės rekomendaciją (Nr. 1)).

## 9. KYC proceso, kai klientas nepilnametis, problematika

Nepilnamečių<sup>8</sup>, neveiksnių ar ribotai veiksnų asmenų klientų bei jų atstovų – vieno iš tėvų, globėjų ar rūpintojų, ryšio (teisės veikti kliento vardu) tikrinimas nėra efektyvus ir apsunkina paslaugų prieinamumą nuotoliniu būdu. Nepilnamečių, neveiksnių ar ribotai veiksnų asmenų atstovavimo taisyklės nustato Civilinis kodeksas ir kiti teisės aktai, todėl FĮ bei kiti įpareigotieji subjektai, prieš užmezdami dalykinius santykius ar jų eigoje, tikrina ryšį (teisę veikti kliento vardu) su vienu iš tėvų, globėjų ar rūpintojų. Siekdamas patikrinti ryšį, atstovas ar tam tikrais atvejais pats klientas turi FĮ ar kitam įpareigotajam subjektui pateikti ryšį patvirtinančius dokumentus (vaiko gimimo liudijimą ar globą, rūpybą patvirtinantį dokumentą).

**Grupės rekomendacija.** Siekiant efektyvinti dalykinių santykių užmezgimą su nepilnamečiais, neveiksniais ar ribotai veiksniais asmenimis ir bendradarbiavimą dalykinių santykių metu, būtų galima sudaryti galimybę gauti vaiko gimimo liudijimo duomenis iš GR, o neveiksnių ar ribotai veiksnų asmenų – iš NRVAR, neprašant nepilnamečių, neveiksnių ar ribotai veiksnų asmenų atstovų ar, tam tikrais atvejais, pačių klientų, patiems pateikti ryšį patvirtinantį dokumentą. FĮ suteikus prieigą prie GR bei NRVAR (vieno langelio principu, kaip pasiūlyta Grupės pateiktame KYC API sprendimo modelyje), būtų didinamas finansinių paslaugų prieinamumas nepilnamečiams, neveiksniams ir ribotai veiksniais asmenims.

Be to, siekdama efektyvinti dalykinių santykių užmezgimą su nepilnamečiais, neveiksniais ar ribotai veiksniais asmenimis, Grupė atkreipia dėmesį į tai, kad rinkoje kai kurios FĮ yra suformavusios praktiką nedubliuoti atstovo tapatybės nustatymo. Tuo atveju, jeigu kliento tapatybė jau yra nustatyta pagal PPTFPĮ 10 ar 11 straipsnio reikalavimus ir jis pareiškia norą užmegzti dalykinius santykius nepilnamečio, neveiksnaus ar ribotai veiksniaus asmens vardu, FĮ nenustatinėja atstovo tapatybės pakartotinai pagal PPTFPĮ 10 ar 11 straipsnio reikalavimus. Tokiu atveju atstovui pakanka elektroniniais kanalais prisijungti prie savo paskyros FĮ, pavyzdžiui, interneto banko, ir pateikti prašymą atidaryti sąskaitą atstovaujamo asmens vardu. FĮ, įsitikinęs, kad atstovas turi teisę atstovauti nepilnamečiui, neveiksniui ar ribotai veiksniaui asmeniui, gauna duomenis, informaciją ar dokumentus, reikalingus nepilnamečio, neveiksnaus ar ribotai veiksniaus asmens tapatybei nustatyti pagal PPTFPĮ 9 ir 12 straipsnius. Toks būdas klientams patogus ir greitesnis, taip pat išvengiama dvigubas atstovo tapatybės nustatymas.

<sup>8</sup> Čia ir toliau nepilnamečiai, kurie nėra emancipuoti.



## 10. KYC procesas BDAR kontekste

KYC procesas yra neatsiejamas nuo klientų duomenų tvarkymo. Iš esmės visi kliento, kuris yra fizinis asmuo, KYC duomenys yra asmens duomenys, taip pat reikšminga dalis klientų, juridinių asmenų, KYC duomenų (pavyzdžiui, vadovų, atstovų, galutinių naudos gavėjų duomenys) yra asmens duomenys. Šie asmens duomenys privalo būti tvarkomi vadovaujantis BDAR ir Asmens duomenų teisinės apsaugos įstatymo nuostatomis. Grupė mano esant reikšminga aptarti kai kuriuos asmens duomenų teisinės apsaugos KYC procese klausimus.

Prieš vertinant reikšmingus KYC API sprendimo aspektus, svarbu atkreipti dėmesį į tai, kad visi sprendime dalyvaujantys subjektai (valstybės registru ir informacinių sistemų valdytojai ir tvarkytojai, KYC API sprendimo valdytojas, FĮ) visus ir bet kuriuos sprendimui reikšmingus asmens duomenis (KYC duomenis) gali ir privalo tvarkyti teisėtais pagrindais. Asmens duomenų teisėto tvarkymo pagrindai yra išvardyti BDAR 6 straipsnio 1 dalyje ir labai apibendrintai galima būtų pasakyti, kad visi sprendime dalyvaujantys subjektai asmens duomenis tvarko bent vienu iš šių pagrindų:

- a. duomenų subjekto (fizinio asmens) sutikimu arba
- b. teisės aktuose nustatytu pagrindu (dažniausiai vykdant teisės aktuose nustatytas teises prievoles arba pavestas viešosios valdžios funkcijas).

Kadangi KYC API sprendimas šiuo metu yra orientuotas tik į universaliuosius duomenis, kurie yra kaupiami ir saugomi valstybės registruose ir informacinėse sistemose, tokių duomenų tvarkymas yra grindžiamas teisės aktais ir tolesnis jų perdavimas FĮ bei tvarkymas KYC tikslais turėtų visų pirma remtis teisės aktuose įtvirtintais pagrindais. Nors duomenų subjekto (fizinio asmens) sutikimas išlieka kaip galimas asmens duomenų tvarkymo teisėtumo pagrindas, Grupės vertinimu, jo detalčiau analizuoti šios ataskaitos kontekste nėra tikslinga. Esminis duomenų subjekto sutikimo kaip duomenų tvarkymo pagrindo trūkumas yra tai, kad duomenų subjektas gali bet kada tokį sutikimą atšaukti. Siekiant sukurti tvarų, efektyvų ir patikimą KYC optimizavimo modelį, toks modelis visų pirma turėtų remtis patikimesniais duomenų tvarkymo pagrindais, t. y. teisės aktuose įtvirtintais pagrindais.

Ataskaitos aiškumo tikslais toliau yra aptariami tik, Grupės nuomone, svarbiausi asmens duomenų tvarkymo momentai. Vis dėlto pažymime, kad visais toliau aptariamais atvejais asmens duomenys privalo būti tvarkomi teisėtais pagrindais ir vadovaujantis teisės aktų reikalavimais. Pavyzdžiui, nors duomenų valdytojas turi teisę savarankiškai nusistatyti asmens duomenų tvarkymo pagrindus, jis privalo nustatyti tik tinkamus ir teisėtus pagrindus, atitinkančius BDAR 6 straipsnio 1 dalies reikalavimus. Be to, valdytojas privalo užtikrinti, kad kiekvienu atveju visą duomenų tvarkymo laiką iš tiesų egzistuoję teisėtas ir tinkamas duomenų tvarkymo pagrindas.

### 10.1. KYC API sprendimo valdytojas: duomenų valdytojas ar tvarkytojas?

Įvertinusi visus privalumus ir trūkumus, Grupė nusprendė, kad šiuo metu tinkamiausias sprendimas KYC proceso efektyvumui didinti yra KYC API sąsajų su viešaisiais registrais sukūrimas, nekuriant atskiros duomenų bazės. Taigi akivaizdu, kad KYC API sprendimas apims asmens duomenų tvarkymą bent jau paimant asmens duomenis iš valstybės registru ir kitų informacinių sistemų ir perduodant juos FĮ. Tikslesnė asmens duomenų tvarkymo apimtis priklausys nuo pasirinkto konkretaus KYC API įgyvendinimo modelio bei tarpinio duomenų tvarkymo poreikio (registro pateiktų duomenų atrinkimo, sisteminimo, siekiant juos perduoti FĮ). Todėl KYC API sprendimo valdytojas ir jo numatoma asmens duomenų tvarkymo veikla turi būti vertinama asmens duomenų teisinės apsaugos tikslais. Svarbu pažymėti, kad *KYC API sprendimo valdytojas* nebūtinai yra ir *duomenų valdytojas* asmens duomenų teisinės apsaugos prasme.

BDAR išskiria *duomenų valdytojus* ir *duomenų tvarkytojus*, kurių pagrindinis skirtumas yra teisė (savarankiškumas) nustatyti duomenų tvarkymo tikslus ir priemones. Duomenų valdytojas savarankiškai nustato, kokius duomenis tvarkys, kaip ir kokiais tikslais juos tvarkys. Pavyzdžiui, registro valdytojas gali nustatyti, kad registre tvarkomi duomenys gali būti perduoti FĮ ir kokia tvarka šie duomenys gali būti perduodami. O duomenų tvarkytojas asmens duomenis tvarko tik taip ir tiek, kiek jam nurodo (suteikia teisę) tokių asmens duomenų valdytojas. Pavyzdžiui, registro valdytojas gali pavesti trečiajam asmeniui – duomenų tvarkytojui nustatyta tvarka ir apimtimi organizuoti ir vykdyti registro duomenų perdavimą FĮ. Tačiau registro tvarkytojas neturi teisės pats savarankiškai nuspręsti teikti duomenis FĮ. Taigi FĮ duomenis gali gauti tiek iš duomenų valdytojo, tiek ir iš duomenų tvarkytojo, jei pastarajam tokią teisę suteikė duomenų valdytojas.

Tokiu pačiu principu sudaromos ir sutartys dėl asmens duomenų teikimo. Duomenų valdytojas savarankiškai sprendžia dėl tokių sutarčių sudarymo. O duomenų tvarkytojas gali sudaryti sutartis dėl duomenų teikimo ir jas vykdyti tik tiek, kiek jam nurodo (suteikia teisę) duomenų valdytojas. Taigi FĮ gali sudaryti sutartis dėl asmens duomenų teikimo su atitinkamų valstybės registru ir informacinių sistemų valdytojais arba su jų tvarkytojais, bet tik jei pastariesiems tokią galimybę numatė atitinkamų registru ir informacinių sistemų valdytojai.

8 lentelė. Duomenų valdytojo ir duomenų tvarkytojo palyginimas

Veiksmas	BDAR	
	Duomenų valdytojas	Duomenų tvarkytojas
<b>Tvarko asmens duomenis</b>	+	+
<b>Savarankiškai sprendžia dėl asmens duomenų tvarkymo (perdavimo)</b>	+	–
<b>Veikia duomenų valdytojo nubrėžtose ribose</b>	–	+
<b>Savarankiškai sudaro sutartis dėl asmens duomenų teikimo</b>	+	–
<b>Sudaro sutartis dėl asmens duomenų teikimo duomenų valdytojo nubrėžtose ribose</b>	–	+
<b>Asmens duomenų tvarkymas turi būti pagrįstas remiantis BDAR 6 straipsnio 1 dalimi</b>	+	+
<b>Asmens duomenų tvarkymo pagrindą tenkina savarankiškai</b>	+	–
<b>Asmens duomenų tvarkymo pagrindą tenkina duomenų valdytojas</b>	–	+

Atsižvelgdama į KYC API sprendimo pobūdį bei siūlomo modelio aprašymą, kuris iš esmės neapima naujos duomenų bazės kūrimo bei asmens duomenų saugojimo, Grupė vertina, kad KYC API sprendimo valdytojas nebus savarankiškas asmens duomenų valdytojas BDAR prasme. Tačiau KYC API sprendimo valdytojas savo funkcijas gali vykdyti įgydamas visų reikiamų valstybės registru bei informacinių sistemų duomenų tvarkytojo statusą.

Šiuo metu daugelio KYC API sprendimui aktualių valstybės registru ir informacinių sistemų tvarkytojas yra RC, kuris įgaliojimus, susijusius su asmens duomenų tvarkymu, įskaitant asmens duomenų perdavimą tretiesiems asmenims, įgyja teisės aktų pagrindu. Grupės manymu, asmens duomenų teisinės apsaugos požiūriu KYC API sprendimą efektyviausiai galėtų įgyvendinti būtent RC, nes jis jau ir šiuo metu yra iš esmės visų šiuo metu prieinamų ir KYC API sprendimui aktualių

valstybės registrų ir informacinių sistemų tvarkytojas. Siekiant užtikrinti tolesnį asmens duomenų tvarkymą KYC API sprendimo įgyvendinimo tikslais, reikėtų tik peržiūrėti ir, esant poreikiui, atitinkamai papildyti RC įgaliojimus atitinkamų valstybės registrų ir informacinių sistemų atžvilgiu.

### **10.2. Sutartis dėl duomenų teikimo**

KYC API sprendimo esmė yra duomenų paėmimas iš efektyviam KYC procesui reikšmingų valstybės registrų ir kitų informacinių sistemų bei šių duomenų perdavimas FĮ. Toks duomenų teikimas FĮ turėtų būti grindžiamas sutartimis dėl duomenų teikimo. Nesant KYC API sprendimo, FĮ tokias sutartis turi sudaryti su kiekvieno registro bei kitų informacinių sistemų valdytojais arba tvarkytojais (jei pastarieji turi tokius įgaliojimus). Grupės nuomone, labai svarbu, kad KYC API sprendimas leistų FĮ gauti duomenis vieno langelio principu, t. y. iš vieno KYC API sprendimo valdytojo pagal vieną sutartį dėl duomenų teikimo. Esminių teisinių kliūčių šiam sprendimui Grupė nemato. Kadangi KYC API sprendimo valdytojas veiks kaip sprendime dalyvaujančių valstybės registrų ir informacinių sistemų duomenų tvarkytojas, jis tiesiog turi įgyti įgaliojimus sudaryti sutartis dėl duomenų teikimo. Tokie įgaliojimai gali būti nustatyti atitinkamuose teisės aktuose, kuriuose reglamentuojama registrų ir informacinių sistemų veikla, arba juos galėtų nustatyti minėtų teisės aktų pagrindu veikiančios registrų ar informacinių sistemų valdytojai arba tvarkytojai (jei pastarieji turi tokius įgaliojimus).

Grupės vertinimu, aptariant sutartis dėl duomenų teikimo sudarymo, KYC API sprendimą efektyviausiai galėtų įgyvendinti taip pat RC. RC jau ir šiuo metu yra iš esmės visų šiuo metu prieinamų ir KYC API sprendimui aktualių valstybės registrų ir informacinių sistemų tvarkytojas, turintis teisę perduoti duomenis tretiesiems asmenims ir tuo tikslu sudaryti sutartis dėl duomenų teikimo. KYC API sprendimo įgyvendinimo tikslais reikėtų tik peržiūrėti ir, esant poreikiui, atitinkamai papildyti RC įgaliojimus atitinkamų valstybės registrų ir informacinių sistemų atžvilgiu, kad RC turėtų teisę sudaryti su FĮ vieną sutartį dėl KYC duomenų teikimo.

**Grupės pozicija.** Kadangi modelį įgyvendinantis subjektas KYC duomenų nekaupytų (nauja duomenų bazė nebūtų kuriama) ir tvarkytų juos tik tiek, kiek reikia duomenims gauti iš viešųjų registrų ir informacinių sistemų ir perduoti FĮ, modelį įgyvendinantis subjektas neįgytų duomenų valdytojo statuso BDAR prasme ir veiktų kaip viešųjų registrų duomenų tvarkytojas. Modelį įgyvendinantis subjektas, veikdamas kaip duomenų tvarkytojas pagal BDAR, gali atlikti visus reikiamus modeliui įgyvendinti asmens duomenų tvarkymo veiksmus, taip pat ir sudaryti vieną sutartį su FĮ dėl duomenų teikimo, jei tokius įgaliojimus jam suteikia viešuosius registrus reglamentuojantys teisės aktai arba jų pagrindu viešųjų registrų valdytojai ar tvarkytojai (jei pastarieji tokius įgaliojimus patys turi). Todėl BDAR kontekste KYC API sprendimo valdytoju paprasčiausia būtų RC, kuris jau dabar veikia kaip iš esmės visų šiuo metu į modelio apimtį patenkančių viešųjų registrų tvarkytojas. Siekiant užtikrinti deramą asmens duomenų apsaugą modelio įgyvendinimo tikslais reikėtų tik peržiūrėti ir, esant poreikiui, atitinkamai papildyti RC įgaliojimus atitinkamų viešųjų registrų atžvilgiu.

### **10.3. Teisė būti pamirštam**

Viena esminių ir išsamių aptariamų asmens duomenų subjektų teisių yra teisė būti pamirštam (BDAR 17 straipsnis), todėl Grupė mano, kad šios teisės įtaka KYC API sprendimui įgyvendinti turėtų būti trumpai apžvelgta. BDAR įtvirtina asmens duomenų subjektų teisę reikalauti, kad asmens duomenų valdytojas nutrauktų jo asmens duomenų tvarkymą ir turimus duomenis ištrintų. Tačiau ši

teisė būti pamirštam nėra absoliuti ir jos įgyvendinimas bei teisinės pasekmės priklauso nuo asmens duomenų tvarkymo pagrindo.

Tuo atveju, jei duomenys yra tvarkomi teisės aktuose įtvirtintais pagrindais (pavyzdžiui, FĮ vykdam joms PPTFPĮ nustatytas teisinės prievolės arba RC įgyvendinant jam priskirtas viešąsias funkcijas), duomenų valdytojas turi teisę duomenis tvarkyti toliau savo teisinės prievolės ar viešosios valdžios funkcijoms vykdyti. Taigi, jei duomenys gauti PPTFPĮ prievolėms vykdyti iš viešųjų registru ar valdžios institucijų, šie duomenys tiek FĮ, tiek ir viešųjų registru bei valdžios institucijų gali būti tvarkomi toliau, kol tam yra pagrindas.

Jei KYC API sprendimą įgyvendinantis subjektas asmens duomenis tvarkytų teisės aktu pagrindu (tokia yra Grupės rekomendacija), teisė būti pamirštam neturėtų teisinių pasekmių tolesniam asmens duomenų tvarkymui ir KYC API sprendimą įgyvendinantis subjektas galėtų toliau tvarkyti asmens duomenis, kiek reikia sprendimui tinkamai įgyvendinti.

Jei sprendimą įgyvendinantis subjektas KYC API funkcijas įgyvendintų ne teisės aktu, o asmens duomenų subjektų sutikimų pagrindu, teisė būti pamirštam galėtų būti įgyvendinama prieš KYC API sprendimo valdytoją. Atsižvelgiant į ribotą tarpinį asmens duomenų tvarkymą KYC API sprendimo dalyje, teisė būti pamirštam visų pirma reikštų, kad nuo duomenų subjekto pareikalavimo su KYC API negalėtų būti teikiami FĮ tokio subjekto asmens duomenys. Vis dėlto teisė būti pamirštam neapribotų FĮ teisės gauti duomenis iš modelyje dalyvaujančių valstybės registru ir informacinių sistemų tiesiogiai, nors tai ir apsunkintų duomenų gavimą, pailgintų duomenų gavimo laiką ir juos pabrangintų. Todėl Grupė pakartotinai pažymi, kad, siekiant sukurti tvarų, efektyvų ir patikimą KYC optimizavimo modelį, toks modelis neturėtų būti grindžiamas duomenų subjektų sutikimais kaip duomenų teisėto tvarkymo pagrindu. KYC API sprendimo valdytojas asmens duomenis turėtų tvarkyti iš valstybės registrus ir kitas informacines sistemas reglamentuojančių teisės aktu kylančiais pagrindais, kaip aptarta ir pirmiau.

FĮ asmens duomenis per modelį įgyvendinantį subjektą gautų ir tvarkytų teisės aktuose nustatytais pagrindais kaip savarankiški duomenų valdytojai, t. y. vykdydami jiems PPTFPĮ nustatytą teisinę prievolę. Todėl, Grupės nuomone, duomenų subjekto teisė atšaukti savo sutikimą dėl duomenų tvarkymo ir prašymas ištrinti jo asmens duomenis neturėtų įtakos tolesniam FĮ jau perduotų duomenų tvarkymui PPTFPĮ tikslais ir laikantis duomenų tvarkymo principų.

**Grupės pozicija.** Teisė būti pamirštam galėtų būti įgyvendinta tik KYC API sprendimą įgyvendinančio subjekto atžvilgiu ir tik jei jis asmens duomenis tvarkytų duomenų subjekto sutikimo pagrindu. Todėl Grupė pažymi, kad, siekiant sukurti tvarų, efektyvų ir patikimą KYC optimizavimo modelį, toks modelis neturėtų būti grindžiamas duomenų subjektų sutikimais kaip duomenų teisėto tvarkymo pagrindu. Grupės nuomone, KYC API sprendimas, kol jis apima tik valstybės registru duomenis, turėtų būti grindžiamas asmens duomenų teisėto tvarkymo pagrindais, kylančiais iš valstybės registrus reglamentuojančių teisės aktu.

## Priedai

### 1 priedas. KYC duomenų šaltiniai

\* duomenų šaltinius valdo RC

#### Fizinio asmens anketa

Duomuo	Esamas duomenų šaltinis	Galimas duomenų šaltinis
<b>Identifikavimas:</b>		
Vardas	Kliento asmens tapatybės dokumentas (leidimas gyventi)	GR*
Pavardė		
Asmens kodas arba gimimo data		
<b>Jei veikiama per atstovą:</b>		
Vardas	Kliento atstovo asmens tapatybės dokumentas (leidimas gyventi)	GR*
Pavardė		
Asmens kodas arba gimimo data		
Atstovavimo pagrindą pagrindžiantis dokumentas ir duomenys, leidžiantys patikrinti jo galiojimo terminą ir įgalintus atlikti veiksmus	Įgaliojimas, gimimo liudijimas, teismo sprendimas	ĮR*, GR*, NRVAR*
<b>KYC universalūs duomenys:</b>		
Asmens dokumento numeris, išdavimo ir galiojimo data, išdavimo vieta; arba leidimo gyventi Lietuvos Respublikoje numeris, išdavimo ir galiojimo data, išdavimo vieta	Kliento asmens tapatybės dokumentas (leidimas gyventi)	GR*, Migracijos departamentas prie Vidaus reikalų ministerijos (toliau – MD)
Pilietybė		
Nuotrauka		
Parašas		
Ar asmuo yra politiškai pažeidžiamas? Jeigu taip: vardas, pavardė, einamos pareigos, institucija, ryšys su klientu.	Klientas, įvairūs šaltiniai	Privačių interesų deklaracijų informacinė sistema
Lėšų ir (arba) turto šaltinis	Banko sąskaitos išrašai, metinės pajamų deklaracijos, kiti dokumentai	SODRA, VMI
Gyvenamoji vieta		GR*
Kontaktiniai duomenys: telefono numeris, el. pašto adresas	Klientas	Klientas
Ar klientui, jo atstovui ar galutiniam naudos gavėjui taikomos finansinės sankcijos?	Klientas, įvairūs šaltiniai	Klientas, įvairūs šaltiniai
<b>Jei veikiama per atstovą:</b>		

Atstovo asmens dokumento numeris, išdavimo ir galiojimo data, išdavimo vieta; arba leidimo gyventi Lietuvos Respublikoje numeris, išdavimo ir galiojimo data, išdavimo vieta	Kliento atstovo asmens tapatybės dokumentas (leidimas gyventi)	MD, GR*
Atstovo pilietybė		
Atstovo nuotrauka		
Atstovo parašas		
<b>Naudos gavėjai:</b>		
Vardas	Klientas	Klientas, GR*, MD
Pavardė		
Asmens kodas arba gimimo data		
Pilietybė		
<b>KYC individualūs duomenys:</b>		
Ar klientas pats naudosis FĮ paslaugomis, ar jis atstovaus kito asmens interesams?	Klientas	Klientas
Išmokos gavėjas (tik gyvybės draudime)		
Dalykinių santykių tikslas ir pobūdis	Klientas	Klientas

#### Juridinio asmens anketa

Duomuo	Esamas duomenų šaltinis	Galimas duomenų šaltinis
<b>Identifikavimas:</b>		
Pavadinimas	JAR išrašas	JAR*
Kodas		
<b>Atstovas:</b>		
Vardas	Kliento atstovo asmens tapatybės dokumentas (leidimas gyventi)	JAR*, GR*
Pavardė		
Asmens kodas arba gimimo data		
Atstovavimo pagrindą pagrindžiantis dokumentas bei duomenys, leidžiantys patikrinti jo galiojimo terminą, veiksmus, kuriems atlikti įgaliojimas išduotas	Įgaliojimas, JAR išrašas	ĮR*, JAR*
<b>KYC universalūs duomenys:</b>		
Teisinė forma	JAR išrašas	JAR*
Registruota buveinė		
Faktinė buveinė		
Registracijos išrašas, jo išdavimo data		
Valdymo struktūra	Klientas, JAR išrašas	Klientas, JAR*, JADIS*
Veiklos pobūdis	Klientas, JAR išrašas	Klientas, JAR*

Ar galutinis naudos gavėjas yra politiškai pažeidžiamas asmuo? Jeigu taip, to asmens vardas, pavardė, einamos pareigos, institucija, ryšys su klientu.	Klientas, įvairūs šaltiniai	Privačių interesų deklaracijų informacinė sistema
Ar klientui, jo vadovui, galutiniam naudos gavėjui ar atstovui taikomos finansinės sankcijos?	Klientas, įvairūs šaltiniai	Klientas, įvairūs šaltiniai
Lėšų ir (arba) turto šaltinis	Klientas	VMI, klientas
Kontaktiniai duomenys: telefono numeris, el. pašto adresas	Klientas	Klientas
<b>Atstovas:</b>		
Atstovo asmens dokumento numeris, išdavimo ir galiojimo data, išdavimo vieta; arba leidimo gyventi Lietuvos Respublikoje numeris, išdavimo ir galiojimo data, išdavimo vieta	Kliento atstovo asmens tapatybės dokumentas (leidimas gyventi)	MD, GR*
Atstovo pilietybė		
Atstovo nuotrauka		
Atstovo parašas		
<b>Vadovas:</b>		
Vardas	JAR išrašas	JAR*, GR*
Pavardė		
Asmens kodas arba gimimo data		MD, GR*
Pilietybė		
<b>Naudos gavėjai:</b>		
Vardas	Klientas	JADIS*, GR*
Pavardė		
Asmens kodas arba gimimo data		MD, GR*
Pilietybė		
<b>KYC individualūs duomenys:</b>		
Ar klientas pats naudosis FĮ paslaugomis, ar jis atstovaus kito asmens interesams?	Klientas	Klientas
Dalykinių santykių tikslas ir pobūdis	Klientas	Klientas

**2 priedas. Politiškai pažeidžiami asmenys pagal PPTFPI**

<b>Duomuo</b>	<b>VTEK</b>	<b>VMI</b>	<b>VRK</b>
---------------	-------------	------------	------------

<b>Politiškai pažeidžiami (paveikiami) asmenys pagal PPTFPI</b>	<b>Svarbios viešosios pareigos</b>	valstybės vadovas, vyriausybės vadovas, ministras, viceministras arba ministro pavaduotojas, valstybės sekretorius, parlamento, vyriausybės arba ministerijos kancleris	taip	taip	taip	
		parlamento narys	taip	taip	taip	
		aukščiausiųjų teismų, konstitucinių teismų ar kitų aukščiausiųjų teismo institucijų, kurių sprendimai negali būti skundžiami, narys	taip	ne	ne	
		savivaldybės meras, savivaldybės administracijos direktorius	taip	taip	taip	
		aukščiausiosios valstybių audito ir kontrolės institucijos valdymo organo narys ar centrinio banko valdybos pirmininkas, jo pavaduotojas ar valdybos narys	taip	taip	ne	
		valstybės įmonės, akcinės bendrovės, uždarnosios akcinės bendrovės, kurių akcijos ar dalis akcijų, suteikiančių daugiau kaip 1/2 visų balsų šių bendrovių visuotiniame akcininkų susirinkime, priklauso valstybei nuosavybės teise, valdymo ar priežiūros organo narys	taip	taip	ne	
		savivaldybės įmonės, akcinės bendrovės, uždarnosios akcinės bendrovės, kurių akcijos ar dalis akcijų, suteikiančių daugiau kaip 1/2 visų balsų šių bendrovių visuotiniame akcininkų susirinkime, priklauso savivaldybei nuosavybės teise ir kurios laikomos didelėmis įmonėmis pagal Įmonių finansinės atskaitomybės įstatymą, valdymo ar priežiūros organo narys	taip	taip	ne	
		politinės partijos vadovas, jo pavaduotojas	taip	taip	taip	
		ambasadorius, laikinasis reikalų patikėtinis, nepaprastasis pasiuntinys ir įgaliotasis ministras ar aukšto rango ginkluotųjų pajėgų karininkas	ne	taip	ne	
		tarptautinės tarpvyriausybines organizacijos vadovas, jo pavaduotojas, valdymo ar priežiūros organo narys	ne	ne	ne	
		politinės partijos valdymo organo narys	ne	ne	taip	
		<b>Artimieji šeimos nariai</b>	sutuoktinis	taip	taip	ne
			partneris	taip	taip	ne
	tėvai		ne	ne	ne	
	broliai ir seserys		ne	ne	ne	
	vaikai		ne	taip <sup>9</sup>	ne	
	vaikų sutuoktiniai, partneriai		ne	ne	ne	

<sup>9</sup> Pagal Gyventojų turto deklaravimo įstatymą, deklaruojamas vaikų iki 18 arba 24 metų turtas.



	<b>Artimi pagalbin inkai</b>	asmuo, kuris su politiškai pažeidžiamu asmeniu (esamu ar buvusiu) yra to paties juridinio asmens ar juridinio asmens statuso neturinčios organizacijos dalyvis arba palaiko kitus dalykinius santykius	ne	ne	ne
		asmuo, kuris yra vienintelis juridinio asmens ar juridinio asmens statuso neturinčios organizacijos, įsteigtos ar veikiančios <i>de facto</i> siekiant turtinės ar kitokios asmeninės naudos politiškai pažeidžiamam asmeniui (esamam ar buvusiam), naudos gavėjas	ne	ne	ne