FINANŠU NOZARES ASOCIĀCIJA

Doma laukums 8A-6, Rīga, LV-1050
Reģ. Nr. 40008002175
Tālrunis: 67284528
info@financelatvia.eu
www.financelatvia.eu

RĪGĀ

2019. gada 28. jūnijā
Nr. 1-23/111_e

Finanšu ministrijai
pasts@fm.gov.lv

Par klientu izpētes rīku platformu (KYC utility)

Finanšu nozares asociācija (turpmāk – Asociācija) ir minēta kā viena no līdzatbildīgajām institūcijām Ministru kabineta 2018. gada 11. oktobra rīkojuma ''Par Pasākumu plānu noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanai laikposmam līdz 2019. gada 31. decembrim'' (turpmāk – *Moneyval* plāns) 4.10. punkta, kas paredz sagatavot izvērtējumu par nepieciešamo normatīvo aktu grozījumiem klienta izpētes rīka (*KYC utility*) izveidei, kas ļautu likuma subjektiem izmantot klientu izpētes informāciju, ko ieguvuši citi likuma subjekti, izpildei.

Asociācija, pamatojoties uz *Moneyval* plāna 4.10. punktu, ir sagatavojusi izvērtējumu par klientu izpētes rīku platformu (*KYC utility*). Nosūtām apskatu par klientu izpētes rīku platformu pielikumā un aicinām Jūs organizēt tālāku šī izvērtējuma un priekšlikumu apspriešanu un virzību sadarbībā ar uzņēmējus pārstāvošajām organizācijām, kuru biedriem piekļuve šādam rīkas ir būtiska efektīvai risku vadība un kopīgi nodrošinot efektīvu cīņu ar finanšu un ekonomiskajiem noziegumiem.

Pateicamies par līdzšinējo veiksmīgo sadarbību un ceram uz turpmākām auglīgām diskusijām. Esam gatavi tajās piedalīties, lai turpinātu darbu pie *KYC utility* ieviešanai nepieciešamā tiesiskā regulējuma izstrādes.

Pielikumā: Apskats par klientu izpētes rīku platformu (*KYC utility*) uz 20 lapām.

Ar cieņu

valdes priekšsēdētāja Sanda Liepiņa

ŠIS DOKUMENTS IR ELEKTRONISKI PARAKSTĪTS AR DROŠU ELEKTRONISKO PARAKSTU UN SATUR LAIKA ZĪMOGU

K. J. Īvāns, karlis.ivans@financelatvia.eu

FINANŠU NOZARES ASOCIĀCIJA

Doma laukums 8A-6, Rīga, LV-1050
Reģ. Nr. 40008002175
Tālrunis: 67284528
info@financelatvia.eu
www.financelatvia.eu

RĪGĀ

2019. gada 28. jūnijā

APSKATS
par klientu izpētes rīku platformu (*KYC utility*)

[1] Tvērums

Šis apskats vērtē iespēju izveidot tiesisko regulējumu, lai dotu iespēju uzņēmējiem, tajā skaitā NILLTFNL likuma subjektiem, uzsākt dalīšanos ar saviem *KYC* (*know your customer*) datiem, ievietojot tos platformā, ārpus konsolidētās grupas ietvara (turpmāk – ***shared KYC Utility***).

Pasaulē ir aktuāli uzlabot klientu izpētes sistēmas un veidot platformas, kurās notiek dalīšanās ar informāciju, lai stiprinātu spēju novērst ar NILLTF saistītos riskus. Katra valsts un katrā reģionā esošās finanšu institūcijas izvēlas sev visērtākos risinājumus, kas kopumā tos padara individuālus, tāpēc katrai valstij ir svarīgi kopā ar nozari un iespējams lielo uzņēmumu pārstāvjiem pieņemt lēmumu par to, kā vislabāk veidot *shared KYC utility*, lai sasniegtu visaugstākos atbilstības standartus, līdz ar to uzlabotu valsts reputāciju citu valstu starpā un mazinātu kopējās klientu izpētes izmaksas.

Ministru kabineta 2018. gada 25. septembra plāna ''Pasākumu plāna noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanai laika periodam līdz 2019. gada 31. decembrim'' 4.10. punkts paredz, ka *KYC Utility* izveide var būt viens no risinājumiem. Pie šī punkta Finanšu nozares asociācija ir norādīta kā viena no atbildīgajām organizācijām.

2018. gada 3. decembra sēdē Finanšu nozares asociācijas padome uzdeva Finanšu nozares asociācijas valdei izvērtēt iespēju izveidot *shared KYC Utility*, līdz ar to ir sagatavots šāds apskats. Šis apskats ir nepieciešams arī tāpēc, lai ideju par *shared KYC Utility* uzturētu aktuālu attiecībās ar valdību, akcentējot tās kā politiskas iniciatīvas nozīmību.

Apskats tika izsūtīts Asociācijas Juridiskajai komitejai, Darbības atbilstības un kontroles komitejai, kā arī GDPR darba grupai. Saņemtie ieteikumi ir iekļauti šajā apskatā.

Šis apskats ir uzskatāms par politikas dokumentu, kas sniedz īsu pārskatu par tematu un satur apsvērumus un ieteikumus, kuriem nav galēja rakstura un kuri ir paredzēti turpmākai apspriešanai pēc to iesniegšanas Finanšu ministrijā.

Šis apskats nav par jebkāda konkrēta *shared KYC Utility* izveidi.

[2] Iepazīstināšana ar modeli

Priekšlikumi šajā apskatā paredz, ka saskaņā ar Latvijā šobrīd spēkā esošo regulējumu ir četri veidi, kādos likuma subjektu ir tiesīgi dalīties ar klienta izpēti saistīto informāciju:

1) informācijas apmaiņa starp pusēm, īstenojot vienu transakciju;
2) informācijas apmaiņa konsolidētas grupas ietvarā;
3) privātā-privātā dalīšanās ar informāciju par klientiem, ar kuriem darījuma attiecības tika pārtrauktas vai tika atteikts tās nodibināt, ņemot vērā NILLTF apsvērumus;
4) publiskās-privātās informācijas dalīšanās partnerības līdzīgas UK JMLIT.

Turklāt šis apskats ņem vērā to, ka kredītiestādēm ir arī tiesības piekļūt dažādiem publiskiem reģistriem (iedzīvotāju, automašīnu, nederīgo dokumentu, Valsts ieņēmumu dienesta, zemesgrāmatu) bezmaksas, lai īstenotu *KYC* procesus, kā arī izmantot licencētus kredītinformācijas birojus kā vienotas piekļuves kanālu.

PNP (politiski nozīmīgo personu) reģistrs likuma subjektiem būs pieejams no 2019. gada augusta.

Shared KYC Utility nav paredzēts kā "supersistēma", kas nosegtu visus KYC procesus, pārdalītu atbildību vai izveidotu visiem derīgu risinājumu/modeli.

Likuma subjekti var izveidot *shared KYC Utility*, nododot uz ārpakalpojumu kādu no KYC procesa posmiem, šādam modelim nebūtu nepieciešama licence, izņemot saskaņošanas, kuras pieprasa konkurences jomas normatīvie akti. Šādu modeli varētu raksturot kā privātu *KYC Utility*. **Šāds *Shared KYC Utility* modelis ir vairāk raksturīgs banku sektoram ar standartizētiem procesiem** (piemēram, Nordic KYC projekts).

Shared KYC Utility vai daļa no tā var tikt veidota kā kanāls caur kuru iegūt informāciju no publiskiem reģistriem vai izmantot to, lai identificētu klientu vai izveidotu klienta profilu, ar kuru pēc tam dalīties ar citiem likuma subjektiem identifikācijas nolūkos (parasti pēc klienta pieprasījuma). Šāds *KYC Utility* modelis prasītu piekļuvi publiskiem reģistriem un visvairāk būtu piemērots privātpersonām to identificēšanai un pamatinformācijas iegūšanai. Šajā ziņā pastāvētu līdzība ar atsevišķiem Singapūrā pastāvošajiem modeļiem, par ko minēts tālāk tekstā.

Shared KYC Utility galvenokārt būtu paredzēts, lai vairāki savstarpēji nesaistīti likuma subjekti dalītos ar būtisko klientu izpētes laikā iegūto informāciju. Šis apskats nenosaka, kas ir būtiskā informācija, ar kuru jādalās, to noteiktu Ministru kabineta noteikumi, ņemot vērā jomas ekspertu ieteikumus. Šāds *shared KYC Utility* piedāvātu saviem klientiem informāciju kā pakalpojumu. Piemēram, dotu piekļuvi būtiskai daļai no KYC anketas, sniegtu informāciju par to, vai persona nav iekļauta kādā sarakstā (piemēram, sankciju sarakstā), norādītu, vai persona nav uzskatāma par augsta riska personu (piemēram, PNP).

Līdz ar to pēdējā aprakstītajā modelī *shared KYC Utility* darbojas līdzīgi kā kredītinformācijas birojs (nodrošina daļu no informācijas, kas nepieciešama aizdevuma izsniegšanas procesā), **galvenokārt ir svarīga ne-banku sektoram**. Šajā aspektā apskats piedāvā fokusēties uz tāda tipa *shared KYC Utility*, kas pieejams tikai uzņēmumiem un privātpersonām, kas saistītas ar uzņēmumiem un privātpersonām. Tādējādi šādam *shared KYC Utility* būtu jāsaņem licence.

Informācijas apmaiņai starp dažādiem *shared KYC Utility* ir jābūt iespējamai un tas ir atkarīgs no tā, vai likuma subjekti būs ieinteresēti to ieviest.

Šis priekšlikums neapsver pienākumu obligāti piedalīties jebkāda veida *shared KYC Utility*.

Apskats nepiedāvā regulēt tādus KYC rīkus, kas ir pieejamas tirgū un piedāvā informācijas apkopošanu no publiski pieejamiem avotiem, vai tādu rīku, ar kurš paredzēts visu kredītiestāžu transakciju analīzei (Nīderlande).

[3] Nepieciešamība

Moneyval savā ziņojumā norāda, ka Latvijai ir virknē jomu, kas saistītas ar Noziedzīgi iegūtu līdzekļu legalizāciju un terorisma finansēšanas (turpmāk – **NILLTF**) risku identificēšanu un novēršanu, jāveic būtiski uzlabojumi .[1]

Ministru kabineta 2018. gada 25. septembra sēdē apstiprinātais plāns *Moneyval* ieteikumu ieviešanai līdz 2019. gada 1. martam paredz "sagatavot izvērtējumu par nepieciešamo normatīvo aktu grozījumiem klienta izpētes rīka (*KYC utility*) izveidei, kas ļautu likuma subjektiem izmantot klientu izpētes informāciju, ko ieguvuši citi likuma subjekti".[2]

Ir vispāratzīts, ka ekonomikas labai funkcionēšanai ir nepieciešama atbilstoša risku kultūra. Kredītriska vadībai masveida informācijas apstrāde par kredītņēmējiem ir vispārpieņemta un regulēta. Mūsdienās ar NILLTF un starptautiskajām sankcijām saistīts risks ir ar vēl lielāku nozīmi, un tādēļ ir jārod mehānisms kā šādu informāciju pietiekamā veidā apkopot un izmantot.

Valstīs, kurās izveidots *KYC utility*, tiek atzīts, ka "pazīsti savu klientu" prasība ir izteikti "sāpīgs jautājums" no regulatorā un operacionālā risku un izdevumu, kā arī klienta skatupunkta. Personām, kas vēlas pašas izmantot vai palīdz finanšu sistēmu izmantot prettiesiskiem mērķiem ir lieliskas iespējas izmantot atšķirības atbildīgo likuma subjektu un citu uzņēmumu, kuriem jānodrošina un kuri nodrošina, lai minētās personas nevarētu netraucēti piekļūt finanšu sistēmai, informācijas pieejamībā. *KYC utility* ir rīks, lai to novērstu,[3] un ļautu no risku neuzņemšanās vai atteikšanās no riskiem pāriet uz kvalitatīvāku un atbilstošu risku pārvaldību.

[4] *Shared KYC utility* tvērums

Katram Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanas likuma (turpmāk – **NILLTFNL**) subjektam (*obliged entity)* ir jāveic klienta identifikācija un izpēte pirms darījuma attiecību uzsākšanas, kā arī darījuma attiecību uzturēšanas laikā, papildus veicot arī darījumu (transakciju) uzraudzību. *KYC* - **pazīsti savu klientu** - ietver visu šo pasākumu kopumu klienta, viņa biznesa un sadarbības partneru pārzināšanai.

---

[1] Sīkāk sk. Latvia Fifth Round Mutual Evaluation Report. Moneyval, Strasbourg, 2018. Pieejams: https://rm.coe.int/moneyval-2018-8-5th-round-mer-latvia/16808ce61b

[2] Pasākumu plāns noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanai laika periodam līdz 2019. gada 31. decembrim, 3.2. punkts. Pieejams: https://likumi.lv//ta/id/302218?&search=on

[3] INDUSTRY BANKING KYC UTILITY PROJECT AFTER-ACTION REPORT – KNOWLEDGE SHARING. The Association of Banks of Singapor. Pieejams: https://abs.org.sg/docs/library/kyc-aar_15-nov-2018.pdf

Lai šo uzdevumu varētu pilnvērtīgāk veikt, tiek izstrādāti informācijas tehnoloģiju rīki (turpmāk - IT), kas vienā platformā importē datus no vairākiem avotiem - gan publiski pieejamiem, gan nepieejamiem, gan valsts uzturētiem, gan privātiem, gan paša klienta sniegto informāciju.

KYC Utility var būt tāds, kas darbojas tikai ar klientu darījumiem viena likuma subjekta vai komercsabiedrību grupas ietvaros, gan būt kā datu agregators, kas nodrošina datu apmaiņu un salīdzināšanu bez to uzkrāšanas. Tomēr tikai **individuāls risinājums** viena likuma subjekta līmenī, lai arī var pastāvēt, nedod būtiskāko pienesumu sabiedrībai kopumā. Iespējami ir abi modeļi – gan **centralizēta datu krātuve** vai **decentralizēts datu apstrādes rīks** -, vērtējot konkrētā izstrādātāja risinājumu, normatīvo aktu prasības un personas datu aizsardzības noteikumus.

Abi šie modeļi var būt kombinēti. Piemēram, arī kredītinformācijas birojos daļa informācija ir vienotā datu bāzē, bet daļu informācijas iegūst tikai tūlītējas padošanas vajadzībām un/vai reitinga veidošanai.

Neatkarīgi no datu apstrādes rīka darbības modeļa, ir skaidrs, ka tas prasīs drošu datu apmaiņas kanālu izveidi, mašīnlasāmu datu struktūru, kā arī vienotu tehnisko standartu paredzēšanu gan valsts, gan privātajā sektorā (tostarp API). Tādēļ būtu ieteicams, ka tiek ieviests vienots kanāls (agregators) valsts reģistru datu padošanai.

[5] Informācija apmaiņa

NILLTF risku efektīvai pārvaldībai ir nepieciešama vairāku likuma subjektu un valsts institūciju sadarbība, apmainoties ar informāciju, kas var tikt raksturots kā *private - private vai public - private information sharing*. Šobrīd NILLTFNL paredz ierobežojumus informācijas apmaiņai vai informācijas ieguvei, pamatā fokusējoties uz informācijas apmaiņu konkrētās individuālas transakcijas gadījumam.

NILLTFNL īsumā nosaka, ka tikai finanšu iestādēm ir noteikti saprātīgi informācijas apmaiņas kanāli. Tikai finanšu iestādes var savstarpēji atzīt klienta izpēti un apmainīties ar datiem par to (29. pants, Kredītiestāžu likuma 62. panta astotā daļa), sniegt informāciju korespondentbankām (44. pants) vai citām finanšu iestādēm konkrētu darījumu ietvaros (38. pants), bez maksas piekļūt virknei valsts reģistru (41. pants), kā arī apmainīties ar datiem par klientiem, ar kuriem darījuma attiecības ir izbeigtas vai nav uzsāktas NILLTF risku dēļ (44. pants). Atsevišķi likuma subjekti var izpaust ziņošanas Finanšu izlūkošanas dienestam (turpmāk – FID) faktu noteiktu darījumu gadījumā (38. pants), kā arī iegūt datus no Uzņēmumu reģistra (5.[1] pants). Visi likuma subjekti ir tiesīgi apmainīties ar informāciju savstarpēji un ar valsts iestādēm FID **Sadarbības koordinācijas grupas ietvaros** (55. pants).

Tātad visu likuma subjektu iespējas iegūt informāciju un apmainīties ar to šobrīd ir ierobežotas. Šobrīd nodrošināt infrastruktūru, lai katrs no tiem varētu piedalīties informācijas iegūšanā, analīzē un apmaiņā ir praktiski sarežģīti gan no datu drošības, gan resursu, gan atšķirīgās ieinteresētības noteiktu datu iegūšanā un tālākā izmantošanā dēļ. Tādēļ ir nepieciešami juridiski un tehnoloģiski rīki, kas to var risināt.

Valstis tiek iedrošinātas pašas novērtēt, cik noderīgi tām būtu brīvprātīgi dalīties ar informāciju, kura pārsniedz *Financial Action Task Force* standartus, lai uzlabotu iespējas identificēt un novērst

iespējamos NILLTF riskus, kā arī pielāgot savus likumus, lai atļautu dalīšanos ar šādu informāciju.[4]

[6] KYC *utility un shared KYC utility*

KYC utility ir viens no rīkiem, ko var izmantot efektīvākai informācijas apmaiņai, paceļot no *case by case basis* uz sistēmisku un strukturētu risinājumu. *KYC utility*, kas integrē vairākus individuālus un publiskus datu avotus, nodrošinot informācijas apmaiņas iespējas, dod ieguvumu sabiedrībai kopumā. Var izdalīt vairākus sadarbības līmeņus. Pirmais – runa tikai par vispārpieejamas informācijas strukturēšanu, otrais – saslēgums ar publiskajiem reģistriem, trešais – klienta aizpildīto anketu un informācijas no klienta izpētes apmaiņa, turklāt otrais un trešais līmenis notiktu vairāku likuma subjektu starpā. Tādēļ turpmāk kopā to sauktu par *shared **KYC utility***.

Tas palielina procesu efektivitāti, jo vairākiem likuma subjektiem informācija par vienu un to pašu nav jāiegūst atkārtoti, lai gan tas neatbrīvo likuma subjektus no pienākuma identificēt klientus un noskaidrot pamatinformāciju. Otrkārt, tas būtiski apgrūtina prettiesisku vai aizdomīgu darbību veicējus "migrēt" apkalpošanai no viena likuma subjekta pie cita, izmantojot laiku, kādu vajadzēs citam likuma subjektam, lai identificētu riskus no jauna. Treškārt, tas neierobežojot ar lieliem resursiem apveltītu likuma subjektu iespējas iegūt datus no citiem datu avotiem, tomēr rada platformu iegūto datu atklāšanai arī tādiem likuma subjektiem, kuru resursi ir ierobežotāki,. Platformā ievada datus, kas var būt noderīgi visiem likuma subjektiem. Dati var kalpot arī pretrunīgas informācijas identificēšanai (verifikācijai). Ceturtkārt, *shared KYC utility* ieviešana ļautu visiem likuma subjektiem apmainīties ar to iegūto informāciju, tādējādi samazinot kopējos nepieciešamos ieguldījumus atbilstības funkcijas nodrošināšanā.

Finanšu iestāžu loma, lai cīnītos ar finanšu noziegumiem, ir identificēt, atbilstoši izpētīt un ziņot par aizdomīgām darbībām, lai neatbilstošiem dalībniekiem liegtu pieeju finanšu sistēmai. Informācijas apmaiņas partnerības loma ir iesaistīties šī pienākuma izpildē, izpildīt to efektīvāk ar mazākiem ieguldījumiem pēc iespējas plašam likuma subjektu lokam.[5] Šo funkciju finanšu iestādes jau īsteno, ieguldot tajā būtiskus resursus.

Ar *shared KYC utility* platformas izveidi NILLTF riski kļūtu vieglāk identificējami, jo, ja izpēti būtu veicis viens likuma subjekts un atklājis augstus NILLTF riskus saistībā ar klientu vai viņa darījumiem, tad šis subjekts informāciju nodotu *shared KYC utility* un citi likuma subjekti to varētu izmantot savā darbībā. Tiem nebūtu jāsāk izpēte no ''0'' punkta, tādējādi būtiski ātrāk identificējot un apstādinot aizdomīgi un prettiesiski iegūtu līdzekļu apriti ekonomikā. Tas faktiski nozīmē, ka NILLTFNL subjekti, kuriem nav pieejami būtiski IT un cilvēkresursi, nav objektīvi spējīgi veikt visas vajadzīgās darbības, lai pārliecinātos, ka klients vai viņa darījumi nerada NILLTF risku.

Shared KYC utility platforma ir salīdzināma ar kredītinformācijas birojiem, proti, tās ir datu bāzes, kurās kredītinformācijas lietotāji un atsevišķi valsts reģistri iesniedz informāciju, un kurām piekļūst visi kredītinformācijas lietotāji, kas vienlaicīgi arī sniedz informāciju kredītinformācijas

[4] Guidance on private sector information sharing. FATF, Paris, 2017. p. 25.

[5] Standard Chartered Wants Greater Sharing of Financial Intelligence. Pieejams: https://blogs.wsj.com/riskandcompliance/2018/09/27/standard-chartered-wants-greater-sharing-of-financial-intelligence/

birojiem (informācijas iegūšanas princips: "**Līdzdarbojies un vari saņemt informāciju, nevis tikai to saņemt, nedodot"**). *Shared KYC utility* darbotos pēc līdzīga principa.

***Tātad shared KYC utility* ir klientu izpētes rīks, kas darbojas kā datu krātuve, kuru ar sev pieejamu informāciju un klientu izpētes rezultātiem papildina finanšu institūcijas, citi likuma subjekti valsts iestādes un komersanti, lai pēc iespējas efektīvi identificētu un novērstu iespējamos NILLTF un finanšu noziegumu riskus.**

[7] Iespējamais tiesiskais regulējums

Shared KYC utility platformas, līdzīgi kā kredītinformācijas biroju ieviešanai, ir nepieciešams **tiesiskais regulējums** - datu apmaiņas tiesiskais ietvars.

Ja *shared* KYC *utility* uztur privāto tiesību subjekts, tad viņam jābūt licencētam, ja tas apmainās ar informāciju, kas ietverta valsts reģistros vai iegūta klienta izpētes ceļā. Valstiska uzraudzība pār šādu subjektu ir obligāta (varētu īstenot, piemēram, Datu valsts inspekcija vai FID).

Šādam risinājumam neapšaubāmi būs nepieciešami ne tikai grozījumi NILLTFNL, bet arī atsevišķi Ministru kabineta noteikumi, kas regulētu virkni detalizētu jautājumu (termiņi, licences, informācijas struktūra utt.). Tas plašāk aplūkots šī dokumenta noslēgumā.

[8] Atbildība

Shared KYC utility platforma neatbrīvo likuma subjektu no atbildības par to, vai NILLTF risku pārvaldība ir bijusi pietiekama. Platforma ir tikai efektīvs palīglīdzeklis darba veikšanai.

Ja likuma subjektu starpā ar likumu ir atļauta klienta izpētes atzīšana, ir iespējams modelis, ka attiecīgi likuma subjekti uztur vienu klienta profilu (lietu). Tomēr praksē šāda pieeja – veidot *Shared KYC utility* – kā vienotu platformu klienta izpētei un informācijas uzglabāšanai izrādījās nesekmīga tās nesamērīgo izmaksu dēļ. Tādēļ, ņemot vērā praktiskos piemērus, atbilstošāk to veidot tikai kā specifiskas informācijas apmaiņas rīku, neveidojot vienotus klienta profilus, ar kuriem visi likuma subjekti strādā vienotā vidē.[6]

[9] Vienas pieturas aģentūras princips

Shared KYC utility platforma var būt izmantojama kā vienota darījuma attiecību uzsākšanas platforma (*a single entry point for customer on-boarding).* Uzņēmējs likuma subjektiem kā papildpakalpojumu var piedāvāt klientu identifikāciju (tas parasti gan tiek uzskatīts par risku paaugstinošu faktoru, ja klientu identificē trešās puses aģents) vai kādu no tā posmiem.

Klienta *KYC* anketa, kas aizpildīta pie viena likuma subjekta, automātiski nevar atbrīvot pārējos no pienākuma klientu identificēt un veikt klienta izpēti. Šis ir palīgrīks informācijas noskaidrošanā un pārbaudē. Klientu ērtībai gan būtu pieļaujams, ka klients pats pie vairākiem likuma subjektiem izmanto vienu sagatavi ar tehniskiem datiem.

[6] MAS to shelve 'know-your customer' project due to high costs, work on SME innovation platform. Pieejams: https://www.straitstimes.com/business/banking/mas-to-shelve-know-your-customer-utility-project-due-to-unexpected-high-costs-ravi

Piemēram, Singapūrā tiek atzīts, ka *shared KYC utility* nedrīkst saskarties ar klientu pats; to dara likuma subjekti.[7]

Šāds princips būtu jāietur arī Latvijā. Tas pats attiektos uz tiesībaizsardzības iestāžu tiesībām piekļūt informācijai, tā būtu iegūstama no likuma subjektiem tieši. FID būtu tiesīgs iegūt datus tieši no platformas, kā arī analizēt tendences klientu struktūrā, savlaicīgi identificētu problēmjautājumus.

[10] Dalīšanās ar datiem: tiesības vai pienākums

Likumā nepārprotami jānosaka, vai dalība *shared KYC utility* būtu likuma subjekta tiesības vai pienākums. Iespējams, ka dažiem likuma subjektiem to paredz kā pienākumu, bet citiem – kā tiesības. Ja kādā daļā tiek paredzēts pienākums, Ministru kabineta noteikumos jānosaka arī cenas par datu izmantošanu veidošanas princips, lai nepieļautu, ka likuma subjektam likumā noteikto pienākumu izpildei cits komersants nosaka nesamērīgi augstu maksu.

[11] *Shared KYC utility* un uzņēmēji

Piekļuve *shared KYC utility* būtu jāpiešķir arī uzņēmējiem (piemēram, maziem un vidējiem uzņēmumiem), kuriem gan nebūtu iespēja apstrādāt visu informāciju, bet būtu iespēja vienkāršotā formā, kas izpaustos, piemēram, kā riska skalas attēlojums, noskaidrot, vai viņu sadarbības partneris vērtējams kā paaugstināta riska komersants un līdz ar to nolemt ar šādu komersantu nesadarboties vai sadarboties, saņemot noteikta veida apliecinājumus vai garantijas. Ja uzņēmēji ierobežotu sadarbību ar paaugstināta riska komersantiem, kā arī paši labāk identificētu un pārvaldītu riskus, kas saistīti ar šādu sadarbību, tad arī likuma subjektiem, it īpaši, finanšu iestādēm būtu jāiegulda proporcionālāki resursi darījumu uzraudzībai, kā arī šādi tiktu stiprināta un uzņēmējdarbības vide Latvijā.

Viena no būtiskām informācijas sadaļām, ar ko saskaras uzņēmēji, ir starptautiskās sankcijas, ko dēvē par sektorālajām sankcijām, ko nevar pārbaudīt tikai pēc kāda noteikta saraksta pārbaudes pieejas. Ja likuma subjekti vai citi komersanti būtu identificējuši šādas personas, piesegkompānijas un citas personas, ar kuru palīdzību tiek mēģināts apiet sankcijas netieši, ar šo informāciju varētu dalīties ar citiem caur *shared KYC utility*, tādējādi tos brīdinot.

[12] Pasaules tendences, mācības no tām

Pasaulē šobrīd gan reģionāli, gan kopumā ir aktuāli izstrādāt kvalitatīvu *shared KYC utility* platformu par to liecina: piecas lielākās Ziemeļeiropas bankas šobrīd veido kopīgu *KYC* risinājumu; nesen HSBC banka piekrita pārdot savu atbilstības sistēmu, kas īsteno klientu padziļināto izpēti, ar domu, ka šis risinājums aptver gan korporatīvos, gan institucionālos klientus un līdz ar to piedāvāt kā pakalpojumu, kas būtu pieejams arī citām finanšu institūcijām.

Ir vairāki modeļi, kā var darboties *shared KYC utility* platforma. Šobrīd esošās *KYC utility* platformas darbojās kā pilna servisa pakalpojumu sniedzēji, ietverot pārbaudes, ierakstu

[7] INDUSTRY BANKING KYC UTILITY PROJECT AFTER-ACTION REPORT – KNOWLEDGE SHARING. The Association of Banks of Singapor. Pieejams: https://abs.org.sg/docs/library/kyc-aar_15-nov-2018.pdf

uzraudzību vai arī veidā, kurā apmaiņšanās ar informāciju notiek starp dalībniekiem bez platformas izveides vai iesaistes, bet šis modelis rada lielu informācijas dublēšanos.

KYC utility pasaulē dažādas formās darbojas jau aptuveni 5 gadus.

Pastāv vairāki modeļi kā *shared KYC utility* varētu darboties un katra modeļa plusi un mīnusi atšķiras:

- **publisks modelis** – valsts uztur un valstij pieder *shared KYC utility* platforma**,** no tā izriet jautājumi – kā tas tiks uzturēts un ko tas nozīmē attiecībā uz atbildību;
- **publisks - privāts modelis –** piederētu gan valstij, gan privātām sabiedrībām kopīgi. Noskaidrojama tā komerciālā forma attiecībā uz ieguldījumiem un iespējamās peļņas sadali, iespējams, šāds modelis veidojams bezpeļņas formā;
- **privāts –** tas nozīmē, ka tas piederētu vai nu vienai finanšu institūcijai vai īpašai kapitālsabiedrībai (SPV), kas uzturētu šo platformu un piedāvātu to kā pakalpojumu. Ja tā pieder finanšu institūcijai, tad tā nebūtu izmantojama plašākā mērogā un nebūtu iespējams nodrošināt pilnīgu neatkarību.

Singapūrā tika atzīts, ka atsevišķa tiesību subjekta izveide ir atbilstošākais risinājums.[8]

Kopumā izvērtējot, vispiemērotākais būtu publiskās/privātās partnerības (PPP) modelis, jo tas nepiederētu ne kādai nozarei, ne valstij, līdz ar to nodrošinātu neatkarību, kā arī lielāku drošību, jo tam būtu arī valstiska darbības uzraudzība (funkcionālā uzraudzība, licencējams subjekts).

PPP modelis sākotnēji būtu jāorganizē tā, ka valsts uzaicinātu dalībniekus piedalīties un izmēģināt platformu.[9] Jāmin, ka šobrīd pasaulē vairāk ir izplatīti tādi modeļi, kuros valsts nav iesaistīta, proti, finanšu institūcijas vienojas, ka veidos kopuzņēmumu, kurā visas apkopos savu KYC informāciju, līdz ar to atvieglinot klientu izpēti.

Lielākās Ziemeļeiropas bankas – *DNB Bank*, *Danske Bank*, *Nordea Bank*, *Svenska Handelsbanken* un SEB – ir paziņojušas, ka tās veidos *KYC Utility* kā kopuzņēmumu (*joint-venture*). Kopuzņēmums piederēs un to kontrolēs minētas bankas ar nolūku izveidot efektīvu, kopīgu, drošu un izmaksas samazinošu platformu, lai dalītos ar konfidenciālu informāciju par klientiem. Pēc darbības uzsākšanas, *Nordic KYC utility* plāno savus pakalpojumus piedāvāt arī lieliem un vidējiem uzņēmumiem.[10] Pēc pieejamās informācijas var secināt, ka šajā risinājumā nav paredzēts, ka platformu valsts papildinās ar savā rīcībā esošo informāciju. Šis KYC Utility darbosies Ziemeļvalstu reģionā un piedāvās KYC pakalpojumus vairākām bankām un šie pakalpojumi, kas sastāv no informācijas, kas nepieciešama saskaņā ar AML/CFT regulējumu, iegūšanas, pārbaudes un piedāvāšanas klientiem, lai nodrošinātu augstāku atbilstību saskaņā AML/CFT regulējumu.[11]

---

[8] INDUSTRY BANKING KYC UTILITY PROJECT AFTER-ACTION REPORT – KNOWLEDGE SHARING. The Association of Banks of Singapor. Pieejams: https://abs.org.sg/docs/library/kyc-aar_15-nov-2018.pdf

[9] Splitting the bill. The role for shared platforms in financial services regulation. Pieejams: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-thecityuk-splitting-the-bill-the-role-for-shared-platforms-in-financial-services-regulation.pdf

[10] Nordic banks explore shared KYC utility. Pieejams: https://www.finextra.com/newsarticle/32178/nordic-banks-explore-shared-kyc-utility?utm_medium=dailynewsletter&utm_source=2018-6-1&member=63850

[11] http://europa.eu/rapid/press-release_MEX-19-3011_en.htm

Dienvidāfrikā pastāv *shared KYC utility* platforma, kura ir izveidota starp Dienvidāfrikas lielākajām finanšu institūcijām un *Refinitiv* (iepriekšējais nosaukums - *Thomson Reuters)*. Dienvidāfrikas *KYC utility* atvieglina informācijas savākšanu un izplatīšanu. Dienvidāfrikā lielām korporācijām, drošības fondiem, aktīvu pārvaldniekiem un citiem *KYC utility* darbojas kā efektīvs, centralizēts risinājums, lai apmainītos ar *KYC* dokumentiem un informāciju starp vairākām finanšu institūcijām caur drošu un bezmaksas interneta portālu. Galvenais iemesls, kāpēc Dienvidāfrikā šī sistēma darbojas efektīvi ir tāpēc, ka noteikumi, kā jāvāc KYC informācija ir standartizēta starp visām finanšu institūcijām, kas piedalās Dienvidāfrikas *KYC utility*.[12]

2014. gadā Dienvidāfrikas Valsts Banka uzlika sodu 4 lielākajām valstī esošajām bankām aptuveni 8 miljonu *euro* apmērā par to, ka tās nespēja ieviest adekvātas NILLTF novēršanas procedūras un risku politikas. 2016. gadā tika izlemts par labu *KYC utility* izveidei sadarbībā ar *Thomson Reuters (šobrīd – Refinitiv)*, lai spētu efektīvāk cīnīties ar NILLTF, kā arī samazinātu ieguldījumus klientu izpētei.[13] Dienvidāfrikas gadījumā valsts nepapildina platformu ar savā rīcībā esošo informāciju.

Vēl jāmin, ka Āfrikas *Afrexim* banka ir izstrādājusi savu *KYC utility* ar nosaukumu *Mansa*. Ar domu, ka šī platforma sadarbosies ar lielākajām Āfrikas bankām un regulatoriem, nodrošinot plašāko *KYC utility* Āfrikā. Par *Mansa* tika paziņots vien 2018. gada jūlijā līdz ar to nav pieejama plašāka informācija par to, kā *Mansa* veicas ar uzstādīto mērķu sasniegšanu.[14]

2017. gadā Singapūras monetārā iestāde paziņoja, ka tā veidos nacionālo *shared KYC utility* finanšu pakalpojumiem, kas balstīsies uz *MyInfo* identificēšanās pakalpojumu, ko ir izstrādājusi Singapūras Finanšu ministrija.[15] Ar šo Singapūra vēlējās nodrošināt, ka finanšu institūcijas var ievērojami vieglāk uzņemt (*on-board*) un pārbaudīt klientus, izmantojot šo *MyInfo* sistēmu.[16] Platformu bija plānots ieviest līdz 2018. gada beigām, bet jāmin, ka lielo izmaksu dēļ, kā arī tāpēc, ka finanšu institūcijas nav aktīvas ar informācijas papildināšanu sistēmā, jo arī šis process ir sarežģīts un prasa lielus ieguldījumus, platformas izveide ir apstājusies un nav zināms, kad tā tiks pilnībā palaista un nodota lietošanā. Singapūras monetārās iestādes vadītājs *Ravi Menon* ir norādījis, ka lielākie sarežģījumi ir nevis ar fiziskām personām, bet gan juridiskām, jo finanšu institūcijām ir grūti sagādāt visu nepieciešamo informāciju platformai, piemēram, par čaulas kompānijām.[17] Singapūras gadījumā platformas izstrādi uzņēmās valsts, ievērtējot, ka privātas finanšu institūcijas sniegs tai informāciju.

Singapūras modelis, lai arī tas vēl pilnībā nedarbojas, ir vērtējams kā visracionālākais pēc pieejamās informācijas apjoma, vienlaikus atzīmējot, ka tā iecerētais darbības modelis (vienots klienta profils, ar ko vienotā vidē strādā vairāki likuma subjekti) ir dārgs un ambiciozs risinājums, un šajā daļā to varētu neizmantot kā labāko paraugu. Ja Dienvidāfrikas esošajā un Ziemeļeiropas

[12] The South African KYC Service. Pieejams: https://africa.thomsonreuters.com/en/products-services/risk-management-solutions/kyc-as-a-service.html
[13] South Africa leads the way in KYC compliance. Pieejams: https://blogs.thomsonreuters.com/answerson/south-africa-leads-way-know-customer-kyc-compliance/
[14] About *MANSA*. Pieejams: https://ej.uz/e4p1
[15] MAS to roll out national KYC utility for Singapore. Pieejams: https://www.finextra.com/newsarticle/30332/mas-to-roll-out-national-kyc-utility-for-singapore
[16] MAS working closely with local and foreign banks to explore a Banking KYC Shared-Services Utility Pieejams: https://www.opengovasia.com/mas-working-closely-with-local-and-foreign-banks-to-explore-a-banking-kyc-shared-services-utility/
[17] Singapore's KYC utility experiment hits snag: MAS. Pieejams: https://www.businesstimes.com.sg/government-economy/singapores-know-your-customer-utility-experiment-hits-snag-mas

plānotajā modelī ir paredzēts, ka finanšu institūcijas apmainās ar savā rīcībā esošo informāciju, tad Singapūras gadījumā platformā nonāktu gan finanšu institūciju rīcībā esošā informācija par klientiem, gan valsts reģistros esošā informācija, kas mazinātu vienu no būtiskajām *KYC utility* platformu problēmām, proti, informācijas uzticamību. Informācija, kas ir atrodama valsts reģistros ir vērtējama kā uzticamāka nekā tā, kas ir pieejama finanšu institūcijām.

No augstāk minētā var secināt, ka pasaulē pastāv dažādi *shared KYC utility* modeļi – Ziemeļeiropas bankas platformu plāno veidot privātu, Dienvidāfrika platformu ir veidojusi privāti, bet sadarbībā ar starptautisku kompāniju –*Refinitiv*, Singapūrā platformu veido valsts partnerībā ar finanšu institūcijām.

Šobrīd *shared KYC Utility* ideja ir, ka tā varētu palīdzēt finanšu institūcijām veikt klientu izpēti, kā arī samazināt un novērst NILLTF riskus, bet atbildība par klientu izpēti vēl joprojām būtu jāuzņemas finanšu institūcijai. Nākotnē tiek prognozēts, ka *shared KYC utility* platforma pilnveidosies tik tālu, ka varēs notikt atbildības pārnešana, proti, *shared KYC utility* būtu tik pilnveidots un saturētu pietiekami daudz informācijas, lai veiktu klientu izpēti. Līdz ar to finanšu institūcijām vairs nebūtu jāveic novērtējums, kā arī jāuzņemas atbildība, to uzņemtos *shared KYC utility* platforma. Tāds ir šīs platformas visaugstākais un iespējams arī tālākā nākotnē sasniedzamais mērķis.

[13] Pieejamas informācijas apjoms un tvērums

Ieviešot *shared KYC utility*, tā informācijas tvēruma aspektā pirmais lēmums ir par to, vai klienti, saistībā ar kuriem notiek informācijas apmaiņa, ir tikai juridiskas personas un juridiski veidojumi, vai arī tās ir arī fiziskas personas. Ja tie ir tikai juridiskie veidojumi, obligāta būs tikai saistīto fizisko personu datu apstrāde. Ja tās būs arī fiziskas personas, tad jānosaka, vai tās būs visas fiziskas personas, vai tikai ar juridiskajiem veidojumiem saistītas fiziskās personas un arī tādas fiziskas personas, kas rada paaugstinātu risku to politiskā nozīmīguma dēļ, konkrētu NILLTF gadījumu dēļ (sk. piemēram, NILLTFNL 44. pantu) un starptautisko sankciju riska dēļ.

Informācija, kas ir vispārpieejama vai iegūstama saskaņā ar normatīvajiem aktiem, nebūtu regulējama, lai nodrošinātu fleksibilitāti jaunu produktu izstrādē platformas ietvaros.

Shared KYC utility ietvaros neapstrādā visu informāciju, kas iegūta klienta izpētes vai darījumu uzraudzības laikā, bet gan tikai to šīs informācijas daļu, ko iegūs NILLTFNL 11.[1] panta ietvaros, ko būs noteicis Ministru kabinets, vai kura ir vispārpieejama.

Informācijas iegūšanai no valsts reģistriem tiktu piemērota samaksa, kas būtu jānosaka centralizēti (vienota Ministru kabineta noteikta nodeva) un būtu viegli un caurskatāmi administrējama.

[14] Seminārā paustās tēzes

2018. gada 23. novembrī notika seminārs "**Pazīsti savu klientu" principa nodrošināšanai un informācijas apmaiņas partnerībām finanšu noziegumu efektīvākai apkarošanai — "AML/CFT: RegTech & Partnerships".**

Latvijas Tirdzniecības un rūpniecības kameras pārstāvis atzina, ka valstij būtu jāsadarbojas ar uzņēmumiem, lai risinātu AML/CFT problēmas, proti, ne tikai jāpārrauga procedūru ievērošana, bet arī jābūt kā ''aktīvam partnerim''. Uzņēmējiem nav pieejami resursi, lai izveidotu efektīvus personalizētus *KYC utility* instrumentus, nodrošinot, ka uzņēmumi, kuriem ir daudz klientu izpētes datu varētu ar tiem arī dalīties ar citiem uzņēmējiem.

FID vadītāja atzina, ka atbalsta šādas platformas izveides ideju. Viņa pauda, ka biznesa intereses nedrīkst nostādīt kā pirmās, lai īstenotu *shared KYC utility* platformu. Pašam svarīgākajam ir jābūt efektīvai cīņai ar finanšu noziegumiem. Nevar uzskatīt par sabalansētu tādu pieeju, kurā valdība uzliek lielas prasības privātajam sektoram, liekot ieguldīt miljonus atbilstības funkcijas īstenošanai, tomēr nenodrošinot nekādu palīdzību šīs funkcijas efektīvā īstenošanā. *Shared KYC utility* platforma palīdzētu ne tikai lieliem biznesiem, noziegumu apkarotājiem, bet arī mazajiem uzņēmumiem cīņā ar finanšu noziegumiem.

Tieslietu ministrijas valsts sekretāra vietniece norādīja, ka būtiski ir ņemt vērā datu apstrādes riskus. Viņa pauda, ka, "lai arī mēs izvirzām absolūti nepieciešamu mērķi – cīnīties ar ekonomiskajiem noziegumiem, padarīt uzņēmējdarbību caurspīdīgu, – aiz tā mērķa mēs apstrādājam arī tādu cilvēku datus, kuriem nav nekāda sakara ar noziegumiem [..]." Šajā aspektā ir jādomā par datu minimizēšanas principu – uz ko to attiecināt, kā nošķirt aizdomīgākus vai riskantākus klientus.

Nav nekādu šaubu, ka šeit ir vajadzīgs pieņemt likumu. Gan Vispārīgās datu aizsardzības regulas dēļ (piemēram, izņēmumi piekļūt datiem, pārtraukt apstrādi, labot datus). Tā kā vēl viens no veidiem, kā valsts varētu iesaistīties *shared KYC utility* platformā, ir dalīties ar publiskos reģistros pieejamo informāciju. Tas arī ir jāregulē un jādara ar likumu.

[15] Priekšlikuma teksts grozījumiem NILLTFNL likumā:

"44.[1] pants. Kopīgais klienta izpētes rīks

(1) Lai pilnvērtīgi veiktu klienta izpēti un darījumu uzraudzību, pārbaudītu klienta sniegto datu patiesumu, nodrošinot būtiskas sabiedrības intereses efektīvai cīņai ar noziedzīgi iegūtu līdzekļu legalizāciju un terorisma finansēšanu un ņemot vērā šo nelikumīgo darbību radītos apdraudējumus demokrātiskai sabiedrībai un sabiedrības drošībai, šā likuma subjektiem šā likuma mērķu īstenošanai ir tiesības:

1) izmantot kā ārpakalpojumu, lai veiktu pilnu vai daļu no klientu izpētes, nepiemērojot šī panta noteikumus, ja tādējādi netiek pārkāpti Konkurences likuma noteikumi;

2) sniegt un iegūt informāciju no klientu kopējā izpētes rīka pakalpojumu sniedzēja.

(2) Lai sasniegtu mērķus, kas noteikti šā panta pirmās daļas 2. punktā likuma subjekti, izmantojot klientu izpētes rīku platformu, var apstrādāt šādu informāciju:

1) informāciju, kas ir publiski pieejama vai ir atļauta tās atkalizmantošana;

2) informāciju, kuru likuma subjektiem ar kopīgā klienta izpētes rīka starpniecību atļauj iegūt citi ārējie normatīvie akti;

3) informāciju no valsts informācijas sistēmām, kas satur ierobežotas pieejamības informāciju, izņemot informāciju, kura attiecas uz sodāmību un pārkāpumiem un kuru var izmantot likuma subjekti atbilstoši šim vai citiem likumiem;

4) informāciju, kas iegūta, likuma subjektam pildot šā likuma prasības, veicot klienta izpēti, tai skaitā klienta identifikāciju, un tas attiecas uz juridiskām personām vai juridisko personu veidojumiem un tikai tām fiziskajām personām, kuras ar tām ir saistītas.

5) informācija, kuru var apstrādāt, ja ir saņemta personas piekrišana;

6) personas un veidojumi, kuras konstatētas kā pakļautas starptautiskajām sankcijām, bet tieši nav minētas starptautisko sankciju sarakstos (sektorālās sankcijas), un citas personas un veidojumi, kas tiek izmantotas starptautisko sankciju apiešanā.

(2) Kopīgo klienta izpētes rīku kā vienoto piekļuves kanālu var papildus šā panta pirmajā daļā noteiktajam izmantot informācijas apmaiņai, kas paredzēta šā likuma 29. pantā, 38. panta ceturtajā daļā un šā likuma 44. pantā.

(3) Kopīgais klienta izpētes rīks informāciju apstrādā, tostarp ir tiesīgs salīdzināt datus, atspoguļo konstatētās pretrunas.

(4) Kopīgajam klientu izpētes rīkam ir tiesības sniegt pakalpojumus likuma subjektiem un citiem uzņēmumiem, kuri piedāvā tādus pakalpojumus, kuriem ir nepieciešama licence un šajās darbības jomās atbilstoši nacionālajam riska novērtējumam pastāv vidējs vai augsts noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas risks.

(5) Kopīgajam klientu izpētes rīkā esošo informāciju ir tiesības nodot uz citu dalībvalsti, ja to paredz licences noteikumi un tādā gadījumā, ja likuma subjekts no citas Eiropas Savienības dalībvalsts sniedz pakalpojumus vai vēlas sniegt pakalpojumus klientam no Latvijas. Informācija, kas tiek nodota kopīgajam klientu izpētes rīkam, netiek uzglabāta ārpus Eiropas Savienības dalībvalstīm.

(6) Likuma subjektam par informācijas sniegšanu kopīgajam klienta izpētes rīkam neiestājas juridiskā, tajā skaitā civiltiesiskā atbildība. Kopīgais klientu izpētes rīks nedrīkst atklāt likuma subjektu, kurš tam sniedza informāciju saskaņā ar šā panta otrās daļas noteikumiem.

(7) Komersantam, kas nodrošina kopīgo klienta izpētes rīku, kas apmainās ar informāciju saskaņā ar šā panta otrās daļas 2. punktu vai starp likuma subjektiem, kas nav vienas uzņēmumu grupas sastāvā, jāsaņem licence, izņemot gadījumu, ja šis komersants atbilst šā likuma 41. panta ceturtās daļas prasībām.

(8) Gadījumos, kad fiziskas personas dati tiek apstrādāti saskaņā ar šo likumu bez šo personu piekrišanas, datu subjekts nedrīkst pieprasīt datu labošanu, dzēšanu vai liegt tos apstrādāt. Informācija, kas sniegta kopīgajam klientu izpētes rīkam, kopīgais klienta izpētes rīka uzturētās nedrīkst izpaust citādi kā viens saskaņā ar šā panta noteikumiem.

(9) Finanšu izlūkošanas dienests ir tiesīgs piekļūt kopīgā klienta izpētes rīka datiem jebkurā laikā un bez iepriekšējas paziņošanas. Iegūto informāciju Finanšu izlūkošanas dienests drīkst izmantot arī šā likuma 55. panta otrajā daļā noteiktajā sadarbības koordinācijas grupā. Citas valsts institūcijas informāciju iegūst no likuma subjektiem normatīvajos aktos noteiktajā kārtībā, un nedrīkst pieprasīt informāciju tieši no kopīgā klienta izpētes rīka.

(10) Ministru kabinets nosaka:

1) prasības komersanta, kas nodrošina kopīgo klienta izpētes rīku, licencēšanai, informācijas tehnoloģiju risinājumiem, valsts nodevas apmēru licences iegūšanai, prasības licences apturēšanai un anulēšanai, kā arī atbildīgo iestādi;

2) prasības likuma subjektiem un/vai komersantiem kopīgā klienta izpētes rīka izmantošanai;

3) informācijas struktūru saņem un izmanto kopīgā klienta izpētes rīka ietvaros, kā arī informācijas apmaiņas regularitāti;

4) vienotās valsts nodevas apmēru, kādu komersants, kas uztur kopīgo klienta izpētes rīku, maksā reizi ceturksnī par ierobežotas pieejamības informācijas iegūšanu no valsts informācijas sistēmām;

5) šā panta otrajā daļā minētās informācijas glabāšanas termiņus un aktualizācijas prasības;

6) mašīnlasāmo datu apmaiņas standartus un individuālo pieprasījumu apstrādes kārtību."

Regulējums attiecas tikai uz klientiem, kas ir juridiskas personas vai juridiski veidojumi un ar tiem saistītām fiziskām personām (patiesie labuma guvēji, nominālie direktori, valdes locekļi, dalībnieki, nominālie direktori utt.).

Būtu svarīgi paredzēt, ka datu apstrāde attiecas ne tikai uz Latvijas likuma subjektiem, bet arī citu ES valstu likuma subjektiem, ja tie ir *shared KYC utility* klienti sakarā ar to, ka viņi strādā ar klientiem no Latvijas.

[16] Personas datu izmantošanas tiesiskums

Eiropas Cilvēktiesību tiesa (turpmāk – ECT) ir secinājusi, ka naudas atmazgāšana rada ļoti nopietnus draudus demokrātijai.[18]

Satversmes tiesa, aplūkojot starptautiskos un Eiropas Savienības normatīvos aktus noziedzīgi iegūtu līdzekļu legalizācijas novēršanas jomā, atzina, ka parasti NILLTFNL paredzētajiem ierobežojumiem ir leģitīms mērķis – sabiedrības drošības aizsardzība. Šā mērķa labad valstij ir pienākums veikt pasākumus, lai kontrolētu finanšu līdzekļu plūsmu, novērstu noziedzīgi iegūtu līdzekļu legalizāciju un terorisma un organizētās noziedzības finansēšanu, kā arī izvairīšanos no nodokļu maksāšanas.[19]

Noziedzīgi iegūtu līdzekļu legalizācija ir arī korupcijas un organizētās noziedzības veicinošs faktors – jo vieglāka un efektīvāka ir naudas atmazgāšanas shēmu īstenošana, jo augstāks ir korupcijas un arī noziedzības līmenis. Ņemot vērā, ka naudas atmazgāšana arī ekonomiski var ietekmēt jebkuru personu, piemēram, paaugstinoties inflācijai, ļaujot iepriekš minētajām grupām netraucēti legalizēt noziedzīgi iegūtus līdzekļus, sociālās sekas var būt būtiski negatīva sabiedrībai kopumā. Turklāt mūsdienās noziedznieki aizvien aktīvāk izmanto globalizāciju un tehnoloģiju attīstību, lai paātrinātu finanšu līdzekļu pārvedi.[20]

Varētu secināt, ka pastāv ļoti nozīmīga sabiedrības interese noziedzīgi iegūtu līdzekļu legalizēšanas un terorisma finansēšanas novēršanā. Tādēļ arī noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanas rīkiem ir jākļūst efektīvākiem, lai maksimāli samazinātu noziegumu veicēju iespējas savu prettiesisko mērķu īstenošanai izmantot klienta izpētes uzdevumu veikšanai nepieciešamo laiku.

[18] ECT 06.12.2012. spriedums lietā *Michaud pret Franciju* (iesnieguma nr. 12323/11) 123. punkts.
[19] Satversmes tiesas 2009. gada 28. maija sprieduma lietā Nr. 2008-47-01 11. punkts.
[20] Apvienoto Nāciju Organizācijas Narkotiku un Noziedzības biroja (UNODC) tīmekļa vietne. Pieejams: https://www.unodc.org/unodc/en/money-laundering/introduction.html?ref=menuside

Shared KYC utility ieviešana samērīgi ierobežotu personu tiesības uz privātās dzīves neaizskaramību un juridisko personu tiesības uz īpašumu.

Atbilstoši Satversmes 116. pantam personas tiesības uz privātās dzīves neaizskaramību un tiesības uz īpašumu var ierobežot likumā paredzētajos gadījumos, lai aizsargātu citu cilvēku tiesības, demokrātisko valsts iekārtu, sabiedrības drošību, labklājību un tikumību.

Shared KYC utility ietvaros veiktās datu apstrādes leģitīmais mērķis būtu demokrātiskās valsts iekārtas, sabiedrības drošības un labklājības aizsardzība. ECT ir secinājusi, ka noziedzīgi iegūtu līdzekļu legalizācijas novēršanas pasākumiem neapšaubāmi ir leģitīms mērķis Eiropas Cilvēka tiesību un pamatbrīvību aizsardzības konvencijas 8. panta 2. punkta izpratnē.[21] Šī panta noteikumi sasaucas ar Satversmes 96. panta prasībām.

Vienlaikus informācijas iegūšana par juridiskajām personām netieši varētu ietekmēt arī to tiesības uz īpašumu, kas paredzētas Satversmes 105. pantā. Proti, uzlabota informācijas apmaiņa daudziem likuma subjektiem vai citiem komersantiem ļautu uzzināt faktus, par kuriem līdz šim tiem nebija zināms, kā rezultātā sadarbība ar noteikta segmenta juridiskajām personām varētu tikt ierobežota. Tas būtu salīdzināmi ar situāciju, kad viens komersants nesniegs ar kredītrisku saistītu pakalpojumu personai, kurai ir zems kredītreitings.

Shared KYC utility radīšana ievērojami apgrūtinās noziedzīgi iegūtu līdzekļu legalizāciju un terorisma finansēšanu, it īpaši samazinās klientu izpētes laiku, kuru finanšu noziegumu veicēji līdz šim izmanto prettiesisku darbību īstenošanai, kamēr notiek viņu radīto risku identificēšanai. Izpētes rīks ļaus verificēt pretrunīgu informāciju un kopumā uzlabos klienta izpētes uzdevumu veikšanas kvalitāti, efektīvāk novēršot darījumus, kas vērsti uz noziedzīgi iegūtu līdzekļu legalizāciju vai terorisma finansēšanu.

Shared KYC utility nosacīti sastāv no četrām sadaļām:

- vispārpieejamā informācija, kuras apstrādei nevajag atsevišķu regulējumu, tomēr tā tiek minēta, lai netiktu uzskatīts, ka šādu produktu papildus nedrīkst piedāvāt, ja apmainās arī ar ierobežotas pieejamības informāciju;
- ierobežotas pieejamības informācija no valsts reģistriem, tomēr šajā gadījumā *shared KYC utility* neparedz tiesības to iegūt, bet gan tikai piedāvā ērtu formu (kanālu) tās iegūšanai;
- klienta izpētes un darījumu uzraudzības laikā iegūtā informācija, kas normatīvajā aktā būs standartizēta pēc noteiktas formas/satura, un tādēļ tieši šī sadaļa ir tā, kura līdz šim nav bijusi paredzēta un **kurai tiek veikts pamattiesību ierobežošanas novērtējums**;

Pirmo jautājumu nodrošina Latvijā vai ārpus tās reģistrēti uzņēmumi, kas nesaņem licenci, vai arī papildus uz viņiem attiecas Informācijas atklātības likuma prasības par informācijas atkalizmantošanu. Savukārt otro jautājumu nodrošina jau šobrīd noteiktais NILLTFNL 41. panta ceturtajā daļā vai citos likumos, piemēram, likumā "Par nodokļiem un nodevām" par nodokļu informācijas sniegšanu.

Shared KYC utility ieviešanas iemesls nav un tas arī nedrīkst būt tikai ieguldījumu samazināšana. Satversmes tiesa ir secinājusi, ka uzdevumu administrēšanas vienkāršība nevar būt vienīgais

[21] ECT 06.12.2012. spriedums lietā Michaud pret Franciju (iesnieguma nr. 12323/11) 99. punkts.

pamattiesību ierobežojuma pamatojums.[22] Tādēļ sadaļā, par kuru paredzēts pamattiesību ierobežojums, netiek atvieglota piekļuve kaut kādu kategoriju datiem, bet paredzēta jauna informācija, ar kuru līdz šim apmainīties kopumā nebija iespējams.

Izvērtējot pamattiesību ierobežojuma samērīgumu, ir jāpārbauda

- vai izraudzītie līdzekļi ir **piemēroti** leģitīmā mērķa sasniegšanai jeb vai ar izraudzīto līdzekli var sasniegt leģitīmo mērķi;
- vai šāda rīcība ir **nepieciešama** jeb vai leģitīmo mērķi nevar sasniegt ar indivīda tiesības mazāk ierobežojošiem līdzekļiem;
- vai ierobežojums ir **atbilstošs** jeb vai labums, ko iegūst sabiedrība, ir lielāks par indivīda tiesībām nodarīto kaitējumu?

Izvērtējot to, vai izraudzītie līdzekļi ir **piemēroti** leģitīmā mērķa sasniegšanai, Satversmes tiesa pārbauda, vai ar izraudzītajiem līdzekļiem var sasniegt leģitīmo mērķi.[23]

FATF Vadlīnijās par informācijas apmaiņu privātajā sektorā tiek secināts, ka informācijas apmaiņai ir būtiska loma finanšu institūciju, uzraugu un tiesībsargājošo iestāžu darbībā, lai tās efektīvāk spētu novirzīt resursus un izstrādāt inovatīvas metodes cīņā ar noziedzīgi iegūtu līdzekļu legalizēšanu.[24]

Trūkumi informācijas apmaiņas sistēmā var radīt dažādas problēmas un padarīt cīņu ar noziedzīgi iegūtu līdzekļu legalizēšanu neefektīvu. Piemēram, privātā sektora loma noziedzīgi iegūtu līdzekļu identificēšanā bieži vien tiek mazināta sakarā ar ierobežoto informācijas plūsmu. Ja likuma subjektiem vairumā valstu ir aizliegts dalīties ar finanšu noziegumu informāciju savā starpā, tad gadījumā, kad likuma subjekts nolemj, ka aizdomu līmenis attiecībā uz konkrētu klientu ir pietiekami augsts, lai izbeigtu savstarpējās līgumattiecības, aizdomīgais klients turpina savu darbību pie cita likuma subjekta. Nākamajam likuma subjektam tādā gadījumā ir jāsāk klienta izvērtēšana no sākuma, dublējot sākotnēji paveikto, no jauna ievācot tos pašus datus no tās pašas personas, līdz ar to nevajadzīgi aizkavējot noziedzīgi iegūto līdzekļu atklāšanu lēnās reakcijas dēļ.[25]

Piedāvātais 44.[1] pants vienlaikus ļauj sasniegt vairākus mērķus. Pirmkārt, apmainīties ar NILLTFNL piemērošanai nepieciešamo informāciju, apvienojot likuma subjektu resursus cīņai ar finanšu noziegumiem. Otrkārt, samazina no personas atsevišķi iegūstamo datu apjomu pie katra no likuma subjektiem. Tas nodrošina ātrāku reakciju un samazina iespējamību neatklāt aizdomīgus darījumus.

Pamattiesību ierobežojums ir **nepieciešams**, ja nepastāv citi līdzekļi, kuri būtu tikpat iedarbīgi un kurus izvēloties personu pamattiesības tiktu ierobežotas mazāk.[26]

---

[22] Satversmes tiesas 19.10.2017. spriedums lietā 2016-14-01 27.2.-27.3. punkts. Latvijas Vēstnesis, 2017, nr. 209.

[23] sk. Satversmes tiesas 2017. gada 8. marta sprieduma lietā Nr. 2016-07-01 23. punktu

[24] Guidance on private sector information sharing. FATF, Paris, 2017. p. 4.

[25] Maxwell N.J., Artingstall D. The Role of Financial Information – Sharing Partnerships in the Disruption of Crime. Royal United Services Imnstitute for Defence and Security Studies. 2017. p. 4.

[26] Satversmes tiesas 2005. gada 13. maija sprieduma lietā Nr. 2004-18-0106 secinājumu daļas 19. punkts.

Piedāvātais 44.[1] pants paredz starptautiski atpazīstama mehānisma, kas tiek licencēts un kura darbība tiek stingri regulēta, izmantošanu to datu apmaiņai, kas iegūti klienta izpētē un darījumu uzraudzībā. Turklāt runa ir tikai par tiem datiem, kas definēti ārējā normatīvajā aktā.

Pastāv divas hipotētiskas alternatīvas šādam piedāvājumam.

Pirmkārt, neapmainīties ar šādu informāciju. Šādā gadījumā mērķis netiek sasniegts. Bez efektīvas informācijas apmaiņas starp likuma subjektiem NILLTF risku pārvaldība ir maz efektīva – viens likuma subjekts neredz visu situāciju, finanšu noziegumu veicējs turpina noziedzīgo darbību nepamanīts pie cita likuma subjekta. NILLTF gadījumus parasti atklāj *post factum*, bet svarīgi ir, ka pastāv mehānisms, kas ļauj tos novērst. Bez *shared KYC utility* tas nav iespējams.

Otrkārt, specifiskos gadījumos atļaut informācijas apmaiņu tikai noteiktu transakciju gadījumā individuāli starp iesaistītajiem likuma subjektiem. Tomēr arī šajā gadījumā tas parasti nozīmēs novēlotu rīcību, kā arī atstās "vājās vietas", kuras varēs izmantot finanšu noziegumu veikšanai.

Līdz ar to jāatzīst, ka nepastāv citi tikpat efektīvi risinājumi, lai nodrošinātu efektīvu informācijas apmaiņu.

Vērtējot pamattiesību ierobežojuma **atbilstību** samērīguma principam, galvenokārt ir jāizvērtē likumdevēja izmantoto līdzekļu radītās sekas, tas ir, vai tiesību normas piemērošana nenodara indivīda tiesībām un likumiskajām interesēm lielākus zaudējumus, nekā iegūst sabiedrība. Vienlaikus ir jāizvērtē šādas tiesību normas ietekme uz ikvienu personu, kuras intereses tā aizskar.[27]

Lai izvērtētu, vai labums, ko iegūst sabiedrība, ir lielāks par personai ar Satversmes 96. pantā paredzēto tiesību ierobežojumu nodarīto zaudējumu, ir jāizvērtē ierobežojuma atbilstība šādiem datu aizsardzības pamatprincipiem: **tiesiskumam, taisnīgumam, minimalitātei un anonimitātei**.[28]

Jāņem vērā, ka **anonimitātes princips** objektīvu iemeslu dēļ konkrētajā gadījumā nevar tikt attiecināts uz *KYC utility* rīka regulējumu.

Tiesiskuma princips ietver nosacījumu, ka personas datu izmantošana un nodošana citiem mērķiem nekā tiem, kuriem dati sākotnēji iegūti, var notikt tikai saskaņā ar personas piekrišanu vai arī uz likuma pamata.[29]

Shared KYC utility rīka izveide tiktu paredzēta NILLTFNL, līdz ar to nav šaubu, ka dati tiktu izmantoti uz likuma pamata.

Taisnīguma princips prasa, lai informācijas iegūšana un apstrāde notiktu tādā veidā, kas izslēgtu nesamērīgu iejaukšanos datu subjektu privātumā, autonomijā un integritātē.[30] Valsts ir tiesīga uzglabāt tikai tādu personas datu apjomu, kas atbilst datu apstrādes leģitīmajam mērķim, un

[27] Satversmes tiesas 2002. gada 19. marta sprieduma lietā Nr. 2001-12-01 3.1. punkts.
[28] Satversmes tiesas 14.03.2011. spriedums lietā Nr. 2010-51-01 14. punkts. Latvijas Vēstnesis, 2011, nr. 42.
[29] Turpat.
[30] Turpat.

pieprasa pietiekamu tiesību aizsardzības līdzekļu esamību. To pietiekamība ir atkarīga no glabājamo personas datu apjoma, glabāšanas ilguma, datu iznīcināšanas un izmantošanas noteikumiem.[31]

Minimalitātes princips paredz, ka personas datu apstrāde ir aizliegta, ja vien nav nepieciešams sasniegt nozīmīgus un iepriekš skaidri noteiktus datu apstrādes mērķus. Proti, ņemot vērā datu pienācīgas glabāšanas nozīmi, datu izmantošana pieļaujama tikai sevišķi būtisku uzdevumu veikšanai, lai aizsargātu kādas tiesiski nozīmīgas intereses.[32] Minimalitātes principa kontekstā ir jānoskaidro arī tas, vai apstrādājamo datu apjoms atbilst datu apstrādes mērķim. Valstij, apstrādājot attiecīgos datus, ir jāveic nepieciešamie pasākumi, lai pārliecinātos, ka personas dati tiek apstrādāti tikai tādā apjomā, kādā tie patiešām ir nepieciešami.[33]

Minētos principus jāanalizē Vispārīgās datu aizsardzības regulas, tostarp tās 5. pantā ietverto personas datu apstrādes principu[34] kontekstā.

Visupirms nepieciešams norādīt, ka NILLTFNL 44.[1] panta redakcija pamatā attiecas **tikai uz juridiskajām personām.**

Uz fiziskajām personām pants attiecināms tikai gadījumos, kad tās ir saistītas ar juridiskajām personām vai pašas rada paaugstinātu risku, piemēram, ir politiski nozīmīgas personas vai nāk no augsta riska trešās valsts. *Shared KYC utility* rīka ietvaros tiks apstrādāta tikai tāda informācija, kas ir nepieciešama klientu izpētes uzdevumu veikšanai un risku identificēšanai.

Datu subjektu loks, par kuriem informācija tiks apstrādāta, ir izsvērts un ierobežots, lai *shared KYC utility* rīka ietvaros tiktu apstrādāta tikai minimāli nepieciešamā informācija par ierobežotu, paredzamu un pēc konkrētām pazīmēm nosakāmu datu subjektu loku. Netiek apstrādāti īpašu kategoriju dati, izņemot gadījumos, kad to pieļauj likums vai nākotnē pieļaus likums.

Tāpat *shared KYC utility* **nenozīmē, ka visiem likuma subjektiem bez ierobežojuma kļūst pieejami visi valsts reģistros esošie dati**; tas ir tikai kanāls, nevis nosaka tiesības tos iegūt.

Vispārīgā datu aizsardzības regula (turpmāk – VDAR) pati par sevi **neaizliedz *shared KYC utility* ieviešanu projektā piedāvātajā veidolā, tomēr prasa ievērot virkni detalizētu prasību, lai datu apstrādi atzītu par nepieciešamu un samērīgu**. Noziedzīgi iegūtu līdzekļu legalizācijas vai terorisma finansēšanas novēršanu var atzīt par leģitīmu mērķi datu apstrādei un datu subjekta tiesību ierobežošanai. Tas izriet no VDAR, Personas datu apstrādes likuma 19. panta, 23. panta pirmās daļas, 26. panta pirmās daļas un 27. panta pirmās daļas, kā arī no NILLTFNL likuma 44.[1] panta piedāvātās redakcijas, proti, *shared KYC utility* nodrošinās un uzturēs **datu apstrādātāji**.

Personas dati var tikt apstrādāti, par pamatu ņemot vērā to, ka tas ir uz pārzini attiecināms **juridisks pienākums** (atbilstoši VDAR 6. panta 1. punkta c) apakšpunktam). Šis pamats ir izmantojams tikai tādā gadījumā, kad piedāvātais 44.[1] pants uzliek pienākumu rīka

[31] Satversmes tiesas 12.05.2016. spriedums lietā Nr. 2015-14-0103 23.3.1. punkts. Latvijas Vēstnesis, 2016, nr. 92.
[32] Satversmes tiesas 14.03.2011. spriedums lietā Nr. 2010-51-01 14. punkts. Latvijas Vēstnesis, 2011, nr. 42.
[33] Satversmes tiesas 11.10.2018. spriedums lietā Nr. 2017-30-01 18.2.1. punkts. Latvijas Vēstnesis, 2018, nr. 203.
[34] Vispārīgās datu aizsardzības regulas 5. pants definē šādus personas datu apstrādes principus: likumīgums, godprātība un pārredzamība, nolūka ierobežojumi, datu minimizēšana, precizitāte, glabāšanas ierobežojums, integritāte un konfidencialitāte, pārskatatbildība.

nodrošinātājam un NILLTFNL subjektam apstrādāt personas datus, izmantojot *shared KYC utility*. Savukārt 44.[1] panta piektajā daļā minētie NILLTFNL subjekti nevarēs izmantot šo pantu kā pamatu personas datu apstrādei, jo tiem ir tikai tiesības veikt personas datu apstrādi, un šajā gadījumā tās ir pārziņa **leģitīmās intereses** (atbilstoši VDAR 6. panta 1. punkta f) apakšpunktam). Šajā gadījumā NILLTFNL subjektam būs pienākums veikt "līdzsvarošanas testu" atbilstoši "29.panta darba grupas"[35] rekomendācijām, lai izvērtētu, vai pārziņa leģitīmās intereses ir uzskatāmas par svarīgākām par datu subjekta interesēm vai pamattiesībām un pamatbrīvībām, kurām nepieciešama personas datu aizsardzība.[36] Tas pārnesīs uz NILLTFNL subjektu lēmuma pieņemšanas risku par to, vai vērts veikt personas datu apstrādi, jo šiem NILLTFNL subjektiem būs pienākums pierādīt, ka veiktā personas datu apstrāde atbilst visām VDAR prasībām.

Īpašu kategoriju personas datus[37] varēs apstrādāt tikai tad, ja atbilstoši VDAR 9. panta 2. punkta "e" apakšpunktam apstrāde attiecas uz personas datiem, kurus datu subjekts apzināti ir publiskojis (piemēram, ja ir publiski pieejama informācija par personas politisko statusu) vai tikai tad, ja atbilstoši VDAR 9. panta 2. punkta "g" apakšpunktam apstrāde ir vajadzīga būtisku sabiedrības interešu dēļ vai saskaņā ar VDAR 9. panta 2. punkta a) apakšpunktu no kura izriet, ka datu subjekts ir sniedzis tādus personas datus, kuru apstrādei persona ir devusi skaidru un nepārprotamu piekrišanu.

Lai apstrādātu speciālo kategoriju personas datus uz pēdējā minētā pamata, kad attiecīgie personas dati nav pieejami publiski, rīka nodrošinātājam un NILLTFNL subjektiem būs jānodrošina pierādījumi tam, ka bez konkrētajiem personas datiem tiek apdraudētas būtiskas sabiedrības intereses.

AML V. direktīvas 43. pants paredz, ka personas datu apstrādi, pamatojoties uz šo direktīvu, nelikumīgi iegūtu līdzekļu legalizēšanas un teroristu finansēšanas novēršanas nolūkos, kā minēts 1. pantā, uzskata par sabiedrības interešu jautājumu atbilstīgi Eiropas Parlamenta un Padomes Regulai (ES) 2016/679 "Vispārīgā datu aizsardzības regula". Vienlaikus piedāvātais 44.[1] pants neparedz "speciālo kategoriju datu apstrādi", tomēr atsevišķos gadījumos šāda informācija var tikt noskaidrota klienta izpētē (piemēram, politiski nozīmīgas personas piederība politiskajai partijai, informācija par arodbiedrības kā klienta vadību) vai noteikta citos likumos.

Runājot par sodāmības datiem, jāņem vērā, ka sodāmības datu apstrāde var tikt veikta tikai oficiālas iestādes kontrolē vai tad, ja apstrādi atļauj normatīvie akti, paredzot atbilstošas garantijas datu subjektu tiesībām un brīvībām (VDAR 10. pants). Piedāvātais 44.[1] pants aizliedz šādu datu apstrādi.

Rīka nodrošinātājs ir pārzinis attiecībā uz personas datiem tādam nolūkam, kuru tam nosaka 44.[1] panta projekts un plānotie Ministru kabineta noteikumi (tas ir attiecībā uz personas datu uzturēšanu rīkā atbilstoši normatīvo aktu prasībām). Savukārt *shared KYC utility* **lietotājs ir**

[35] 29. panta darba grupa ir neatkarīga Eiropas darba grupa, kas līdz 2018. gada 25. maijam (līdz Vispārīgās datu aizsardzības regulas piemērošanai) risināja jautājumus par privātās dzīves un personas datu aizsardzību.

[36] 29. panta darba grupas 2014. gada 9. aprīļa viedoklis 06/2014 par personas datu apstrādi uz leģitīmo interešu pamata ir pieejams šeit: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Minētais viedoklis, kaut arī sniegts par leģitīmo interešu jēdzienu atbilstoši iepriekš spēkā esošajam regulējumam (Direktīva 95/46/EK), tomēr ir aktuāls arī VDAR kontekstā.

[37] Dati, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību, dalību arodbiedrībās, un ģenētisko datu, biometrisko datu, lai veiktu fiziskas personas unikālu identifikāciju, veselības datu vai datu par fiziskas personas dzimumdzīvi vai seksuālo orientāciju.

pārzinis attiecībā uz personas datu apstrādi, kuru tas veiks, pildot savus ar NILLTFNL uzliktos pienākumus, tostarp klienta izpētes jomā. Personas datu apstrādes lomas noteikšana ir nepieciešama, lai saprastu minēto personu atbildības pakāpi attiecībā uz personas datu apstrādi. Pārzinis ir persona, kura ir atbildīga par visu personas datu aizsardzības prasību ievērošanu.

Piedāvātais 44.[1] pants paredz noteiktus personas datu apstrādes mērķus un tie sasaucas ar Satversmes 116. pantā minētajiem mērķiem.

Personas datu precizitātes princips nosaka, ka personas datiem ir jābūt precīziem un, ja vajadzīgs, atjauninātiem (VDAR 5. panta 1. punkta "d" apakšpunkts). Šī principa īstenošanai arī ir jāveic visi saprātīgi pasākumi, lai nodrošinātu, ka neprecīzi personas dati, ņemot vērā nolūkus, kādos tie tiek apstrādāti, bez kavēšanās tiktu dzēsti vai laboti.

Piedāvātā 44.[1] panta redakcija nenosaka personas datu aktualizēšanas procedūru. Tomēr pants atsaucas uz to, ka personas datu aktualizēšanas prasības noteiks Ministru kabinets.

Iepriekšminētos trīs jautājumus risinās arī Ministru kabineta noteikumi, standartizējot tos informāciju, ar kuru notiek apmaiņa kā ierobežotas pieejamības informāciju, kā arī to aktualizē un nodrošina to precizitāti. Risks par neprecīziem datiem pastāv vienmēr.

Piedāvātā 44.[1] panta astotā daļa neierobežo datu subjekta tiesības uz piekļūšanu minētajai informācijai, bet atceļ tiesības pieprasīt datu apstrādes pārtraukšanu. VDAR 18. un 23. pants atļauj aizliegt izmantot datu apstrādes pārtraukšanas pieprasīšanas tiesību, lai sargātu sabiedrības drošību, kā arī sekmētu noziedzīgu nodarījumu novēršanu, tostarp nodrošinātu aizsardzību pret sabiedriskās drošības apdraudējumiem un to novēršanu. Apstrādātie dati ir par privātpersonām, kas saistītas ar juridiskām personām. Datu apstrāde ir nepieciešama, lai mazinātu NILLTF riskus. Ja personai būtu tiesības pieprasīt pārtraukt datu apstrādi, tad tas pilnībā apdraudētu ieguldījumus NILLTFN novēršanā. Vienlaicīgi VDAR 23. panta 2. punkts pieprasa, ka šādu datu subjekta tiesību ierobežošanas gadījumos, likumam, kas nosaka šos ierobežojumus, ir arī skaidri jānosaka papildus informācija par šiem tiesību ierobežojumiem. Šāda informācija var tikt iekļauta NILLTFNL un/vai Ministru kabineta noteikumos.

ECT ir secinājusi, ka, ja ar privāto dzīvi saistīta informācija tiek ievākta un uzkrāta slepenos reģistros ar mērķi cīnīties pret terorismu, tad valstīm ir liela rīcības brīvība dažādu ierobežojumu noteikšanā. Piemēram, gadījumā, ja ievāktās informācijas atklāšana datu subjektam varētu apdraudēt datu apstrādes mērķi (piemēram, cīņu ar terorismu), tad valsts drošības intereses prevalē pār personas tiesībām uz privātās dzīves neaizskaramību, proti, personas tiesības uzzināt to, kāda informācija un kādā apjomā par šo personu ir savākta un tiek uzglabāta, var tikt ierobežotas.[38]

VDAR 5. panta 1. punkta "e" apakšpunktā paredzētais glabāšanas ierobežošanas princips nozīmē, ka personas datus ir pienākums glabāt veidā, kas pieļauj datu subjektu identifikāciju, ne ilgāk kā nepieciešams nolūkiem, kādos attiecīgos personas datus apstrādā. Piedāvātā 44.[1] panta redakcija nenosaka personas datu glabāšanas termiņus. Tomēr pants atsaucas uz to, ka personas datu glabāšanas termiņus noteiks Ministru kabinets. Ņemot vērā to, ka glabāšanas ierobežošanas

[38] ECT 09.06.2006. spriedums lietā *Segerstedt-Wiberg* un citi pret Zviedriju (iesnieguma nr. 62332/00) 99.-104. punkts.

princips ir viens no personas datu aizsardzības pamatprincipiem, ir jānodrošina atbilstoša personas datu glabāšanas termiņu ieviešana, tos nosakot Ministru kabineta noteikumos, tomēr ņemot vērā, ka glabāšanas termiņi nevar pārsniegt NILLTFNL 37. panta otrajā daļa norādīto termiņu, proti, ja juridiskā persona vairs nav viena likuma subjekta klients, tad piecus gadus pēc darījuma attiecību izbeigšanas vai gadījuma rakstura darījuma datus par saistītajām fiziskajām personām dzēš.

Integritātes un konfidencialitātes princips (VDAR 5. panta 1. punkta "f" apakšpunkts) nozīmē, ka personas datus ir pienākums apstrādāt tādā veidā, lai tiktu nodrošināta atbilstoša personas datu drošība, tostarp aizsardzība pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu, izmantojot atbilstošus tehniskos vai organizatoriskos pasākumus.

Piedāvātais 44.[1] pants šos jautājumus deleģē noteikt Ministru kabinetam. Datus nav atļauts nodot vai glabāt ārpus Eiropas Ekonomikas zonas. Ministru kabinets paredzēs minimālās prasības informācijas tehnoloģiju drošības risinājumiem.

Pamatojoties uz VDAR 35. panta 3. punkta "a" apakšpunkta prasībām rīka nodrošinātājam būs pienākums veikt iekšēju novērtējumu par ietekmi uz datu aizsardzību, jo *shared KYC utility* izmantošana nodrošinās ar fiziskām personām saistītu personisku aspektu sistemātisku un plašu novērtēšanu, kuras pamatā ir automatizēta apstrāde (tostarp profilēšana). VDAR neaizliedz profilēšanu. Tomēr profilēšana piedāvātajā 44.[1] pantā neparedz automatizētu lēmumu pieņemšanu *shared KYC utility* līmenī; informācijas izmantošanas kārtību nosaka katrs pats likuma subjekts.