TARTU ÜLIKOOL

ÕIGUTEADUSKOND

Karistusõiguse osakond

Triin Kihuoja

Isikuandmete kaitse õiguse riived rahapesu ja terrorismi rahastamise tõkestamiseks kohaldatavate hoolsusmeetmete käigus ning õiguslikud alused isikuandmete töötlemiseks krediidiasutustel

Magistritöö

Juhendaja

PhD Andreas Kangur

Tartu
2021

SISUKORD

SISSEJUHATUS

Rahapesu ja terrorismi rahastamise vastane võitlus on viimastel aastakümnetel muutunud Euroopa Liidus (edaspidi ka EL) kui ka väljaspool Euroopa Liitu üha olulisemaks. Sellega seoses on oluliselt muutunud standardid rahapesu ja terrorismi rahastamise tõkestamisel. Käesolevaks ajaks on ilmselge, et hoolsuskohustus, mida rakendati rahapesu ja terrorismi rahastamise tõkestamisel kümme aastat tagasi, ei ole enam ajakohane ega piisav, et tagada finantssektori läbipaistvus. Seda ilmestavad viimasel ajal ilmsiks tulnud nö „rahapesu skandaalid", kus mitmetele tuntud pankadele Euroopas või väljaspool Euroopat on määratud trahve, mis küündivad mitme miljoni euroni. Rahapesu ja terrorismi rahastamise tõkestamise alased rikkumised on nende kaasuste puhul toime pandud ligi kümme aastat tagasi. Näiteks oleks Danske pank pidanud oma protseduurireeglid kehtivate rahapesu vastaste õigusaktidega kooskõlla viima või tuvastama rahapesuriske juba 2007. aastal, mil mitteresidentidest klientide portfell omandati[1].

Finantssektori läbipaistvamaks ning stabiilsemaks muutmiseks on Euroopa Parlament ja nõukogu käesolevaks ajaks vastu võtnud kuus rahapesu ja terrorismi rahastamise tõkestamise ohtu käsitlevat direktiivi. Neist olulisim on neljas rahapesu direktiiv (EL) 2015/849[2] (edaspidi ka rahapesu neljas direktiiv), mille sätted on üle võetud Rahapesu ja terrorismi rahastamise tõkestamise seadusesse[3] (RahaPTS).

RahaPTS § 19 lg 1 järgi peab kohustatud isik kohaldama preventiivseid meetmeid ehk hoolsusmeetmeid mh ärisuhte loomisel, juhuti tehtava tehingu tegemisel või kui on kahtlus, et tegemist võib olla rahapesu või terrorismi rahastamisega. Hoolsusmeetmete kohaldamise käigus tuleb kohustatud isikul mh tuvastada kliendi tehingus osaleva isiku või tema esindaja isikusamasus, tegelik kasusaaja või hankida täiendavat teavet ärisuhte või juhuti tehtava tehingu kohta (RahaPTS § 20 lg 1). Hoolsusmeetmeid kohaldatakse selleks, et tagada Eesti

[1] Finantsinspektsiooni 19.02.2019 juhatuse otsus nr 4.1-1/8 ''Ettekirjutus Danske Bank A/S-le'', lk 7.
[2] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2015/849, 20. mai 2015, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist ning millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 648/2012 ja tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2005/60/EÜ ja komisjoni direktiiv 2006/70/EÜ (rahapesu neljas direktiiv) – ELT L 141. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32015L0849&qid=1610985506334 (17.04.2021).
[3] Rahapesu ja terrorismi rahastamise tõkestamise seadus. - RT I, 21.11.2020, 13.

ettevõtluskeskkonna usaldusväärsus ja läbipaistvus, samuti, et tõkestada Eesti rahandussüsteemi ja majandusruumi kasutamist rahapesuks ja terrorismi rahastamiseks.[4]

Rahapesu ja terrorismi rahastamise vastane võitlus on edukas juhul, kui kohustatud isikutel on piisavalt teavet oma klientide ärisuhete, juhuti tehtavate tehingute, ärimudeli või vara päritolu kohta. Seetõttu peaksid liikmesriigid tagama, et kohustatud isikud koguvad ja hoiavad lisaks põhiteabele, nagu äriühingu nimi ja aadress ning asutamist ja õiguspäraseid omandisuhteid tõendavad dokumendid, ka piisavat, täpset ja ajakohastatud teavet tegelikult kasu saavate isikute kohta[5]. See tähendab, et hoolsusmeetmete täitmiseks kogub ja töötleb krediidiasutus kohustatud isikuna[6] isikuandmeid. RahaPTS § 20 lg 1 p 4 lubab krediidiasutustel koguda täiendavat teavet ärisuhte või juhuti tehtava tehingu kohta, kui krediidiasutus sellest aru ei saa ja teabe kogumine on asjakohane. See kohustus hõlmab endas tehingupoolte isikute tuvastamist füüsilise isiku tasandil ehk nende isikuandmete töötlemist.

Teisalt on Euroopa Liit oluliseks pidanud ka isikute õigust oma isikuandmete kaitsele. 2016 aasta alguses läbiviidud isikuandmete kaitse reformi käigus tugevdati ning ajakohastati 25 aastat kehtinud isikuandmete töötlemise reeglistikku. Reformi keskseks õigusaktiks võib pidada Euroopa Parlamendi ja nõukogu üldmäärust (EL) 2016/679[7] (edaspidi ka GDPR/isikuandmete kaitse üldmäärus). Õigus oma isikuandmete kaitsele tuleneb Euroopa Liidu Põhiõiguste harta artiklist 8, mille kohaselt on igaühel õigus oma isikuandmete kaitsele ning selliseid andmeid tuleb töödelda asjakohaselt ja kindlaks määratud eesmärkidel[8].

Teatavasti peab isikuandmete töötlemine olema seaduslik ning vastama isikuandmete kaitse üldmääruses sätestatud isikuandmete töötlemise põhimõtetele. GDPR-i järgi tuleb isikuandmete töötlemisel tagada, et isikuandmeid kogutakse mh õiguspärastel eesmärkidel ning võimalikult vähe. Siin põrkuvad kaks olulist põhimõtet: rahapesu ja terrorismi rahastamise vastane võitlus, mille raames tuleks koguda võimalikult suurel hulgal andmeid, ning

[4] Finantsinspektsiooni soovituslik juhend ''Krediidi- ja finantseerimisasutuste organisatsiooniline lahend ning ennetavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks'', lk 23. Arvutivõrgus: https://www.fi.ee/sites/default/files/2018-11/FI_AML_Soovituslik_juhend.pdf . (21.04.2021).
[5] (EL) 2015/849, põhjenduspunkt 14.
[6] Rahapesu neljanda direktiivi artikli 2 lg 1 p 1 ning RahaPTS § 2 lg 1 p 2 järgi kohaldatakse direktiivi ning seaduse sätteid krediidiasutustele.
[7] Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27.aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) – ELT L 119. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/?qid=1550757219234&uri=CELEX:32016R0679 (20.04.2021).
[8] Euroopa Liidu Põhiõiguste harta. Arvutivõrgus: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:ET:PDF.

isikuandmete kaitse, mille üheks peamiseks põhimõtteks on, et isikute kohta tuleb koguda võimalikult vähe andmeid. Euroopa Andmekaitseinspektor on oma 23.07.2020 arvamuses asunud seisukohale, rahapesu ja terrorismi rahastamise tõkestamise eesmärgi täitmine ei või tulla isikuandmete kaitse õiguse arvelt.[9] Seega tuleb krediidiasutustel leida tasakaal kahe omavahel põrkuva põhimõtte osas ning järgida proportsionaalsuse printsiipi isikuandmete töötlemisel[10].

Käesoleva magistritöö eesmärk on erinevaid rahapesu vastaseid õigusakte ning isikuandmete kaitse õigusakte analüüsides välja selgitada, millistel alustel ning millises ulatuses on võimalik krediidiasutustel töödelda oma klientide isikuandmeid. Isikuandmete kaitse üldmäärus näeb ette, et isikuandmeid võidakse töödelda juriidilise kohustuse täitmiseks, mis autori arvates seab selged piirid isikuandmete töötlemisele. Isikuandmete töötlemisel juriidilise kohustuse täitmisel peaks töötlemise alus tulenema liikmesriigi õigusaktist või Euroopa Liidu õigusaktist[11]. Siiski on võimalik isikuandmeid töödelda ka õigustatud huvi olemasolul, mis autori arvates võimaldab krediidiasutustel koguda ning töödelda rohkem isikuandmeid, kui juriidilise kohustuse täitmise korral. Kuna õigustatud huvi on avatud mõiste, tuleb iga kaasuse puhul eraldi hinnata, kas isikuandmete töötlemine oli seaduslik või mitte. Seetõttu on töö üheks eesmärgiks ka välja selgitada, milliseid isikuandmeid ning millisel juhul võib krediidiasutus töödelda õigustatud huvi alusel. Samuti soovib autor analüüsi käigus välja selgitada, kas rahapesu ja terrorismi rahastamise tõkestamist reguleerivad õigusaktid võimaldavad krediidiasutustel töödelda isikuandmeid erinevalt isikuandmete kaitse üldmäärusest. Veel soovib autor välja selgitada, kas ja millistes olukordades on isikuandmete kaitse õiguse riived intensiivsemad.

Magistritöö teema on aktuaalne, kuna finantssektorit halvavate ebaseadusliku raha voogude tõkestamise kõrval võimalikult palju teavet kogudes, riivavad krediidiasutused isikute põhiõigust isikuandmete kaitsele. Vajalikust palju rohkem isikute kohta teavet kogudes võib krediidiasutus rikkuda isiku õigusi oma andmete kaitsele. Sellist riivet või rikkumist ei saa

[9] European Data Protection Supervisor, ''Opinion 5/2020 on the European Commission's action plan for a comprahensive Union policy on preventing money laundering and terrorism financing'', 23.07.2020, lk 7. Arvutivõrgus:https://edps.europa.eu/sites/edp/files/publication/20-07-23_edps_aml_opinion_en.pdf (17.02.2021).

[10] De Vido, S., Anti-Money Laundering Measures versus European Union Fundamental Freedoms and Human Rights in the Recent Jurisprudence of the European Court of Human Rights and the European Court of Justice. German Law Journal: 2016. lk 1291. Arvutivõrgus: https://heinonline-org.ezproxy.utlib.ut.ee/HOL/Page?collection=journals&handle=hein.journals/germlajo16&id=1307&men_tab=srchresults (23.04.2021).

[11] (EL) 2016/679, põhjenduspunkt nr 45.

õigustada sellega, et finantssektori asutused pelgavad suuri trahve, mida on rahapesu ja terrorismi rahastamise tõkestamise alaste rikkumiste korral võimalik rakendada. Samuti ei sätesta rahapesu ning terrorismi rahastamise tõkestamise alased õigusaktid kogutavate isikuandmete hulka ega laadi. Isikuandmete töötlemine sõltub ka krediidiasutuse riskiisust ning riskihinnangust, ehk mida kõrgema riskiga kliente krediidiasutus teenindada soovib, seda tugevamad peavad olema hoolsusmeetmed, mis tähendab rohkemate andmete kogumist. Suurema hulga andmete kogumine omakorda aitab kõrge riskiga klientide puhul riske maandada.

Nii rahapesu ja terrorismi rahastamise vastane võitlus kui ka isikuandmete kaitse on Euroopa Liidus viimastel aastatel olnud olulised suunad. Kuna rahapesu ja terrorismi rahastamise tõkestamine näeb ette suures mahus andmete kogumist, mis on täiesti vastupidine põhimõte isikuandmete kaitsele, on tegemist kahe suure väärtuse konfliktiga. Euroopa Liidu Kohtu (edaspidi ELK) menetluses on käesoleval ajal vähemalt kaks eelotsusetaotlust, milles küsitakse rahapesu vastaste meetmete õigustatuse kohta just isikuandmete töötlemisel, eriti isikuandmete avaldamisel[12]. Näiteks näeb neljanda rahapesu direktiivi artikkel 30 lg 3 ette, et liikmesriigid tagavad, et äriühingute tegelike kasusaajate[13] andmed hoitaks näiteks äriregistris või avalikus registris. Just selle kohta on ELK menetluses eelotsuse taotlus, et kas juhul, kui selline register on avalik ja kõigile kättesaadav ning kasusaaja isikuandmed on seal avalikud, on tegemist Euroopa Liidu Põhiõiguste Harta artikli 8 rikkumisega.[14]

Magistritöö on jaotatud kolmeks suuremaks peatükiks. Esimeses peatükis analüüsib autor krediidiasutuste poolt kohaldatavaid hoolsusmeetmeid ning nende eesmärke. Samuti kirjeldab autor hoolsusmeetmete liike selgitades millistel juhtudel tuleb kohaldada üldisi, lihtsustatud või tugevdatud hoolsusmeetmeid. Kuna hoolsusmeetmete kohaldamise ulatus oleneb konkreetse krediidiasutuse riskihinnangust ja -poliitikast, on autor võtnud analüüsi aluseks just selle.

---

[12] Isikuandmete avaldamine GDPR art 4 p 2 kohaselt on isikuandmete töötlemine automatiseeritud või automatiseerimata toiming, muuhulgas isikuandmete levitamine või muul moel kättesaadavaks tegemise teel avalikustamine. Seega on isikuandmete avaldamine isikuandmete töötlemise üks viisidest.

[13] ''tegelikult kasu saav omanik'' neljanda rahapesu direktiivi art 3 p 6 kohaselt on füüsiline isik, kes on kliendi lõplik omanik või kes teda tegelikult kontrollib, ja/või füüsiline isik, kelle nimel tehing või toiming tehakse. Selline isik äriühingu puhul on isik, kes kontrollib või omab juriidilist isikut piisava arvu aktsiate või osade või hääleõiguse või omandiõiguse otsese või kaudse omamise kaudu. Otsene omamine tähendab, et füüsiline isik omab kliendis 25% suurust osalust pluss üks aktsia või üle 25% suutust omandiõigust. Kaudne omamine tähendab seda, et kliendis omab 25% suurust osalust pluss üks aktsia või üle 25% suurust omandiõigust äriühing, mis on füüsilise isiku kontrolli all, või mitu äriühingut, mis on sama füüsilise isiku kontrolli all.

[14] EKo C-601/20 *SOVIM SA vs Luxembourg Business Registers,* Eelotsusetaotlus. Arvutivõrgus: http://curia.europa.eu/juris/showPdf.jsf?text=rahapesu&docid=235961&pageIndex=0&doclang=ET&mode=req&dir=&occ=first&part=1&cid=2395483.

Teises peatükis kirjeldab autor õigust isikuandmete kaitsele, selle sisu ning määratlust õigusaktides. Seejärel analüüsib autor isikuandmete töötlemise eesmärgipärasuse, minimaalsuse ning isikuandmete õiguse printsiipe ning minimaalsuse printsiibi konkurentsi krediidiasutuste kohustusega rakendada hoolsusmeetmeid rahapesu ja terrorismi rahastamise tõkestamiseks.

Kolmandas peatükis analüüsib autor võimalikke õiguslikke aluseid isikuandmete töötlemiseks hoolsusmeetmete rakendamisel krediidiasutuste poolt. Peatüki peamine eesmärk on välja selgitada, kas rahapesu ja terrorismi rahastamise tõkestamise alased õigusaktid sätestavad erinorme isikuandmete töötlemiseks. Kui neist õigusaktidest ei tulene isikuandmete töötlemiseks erinorme, analüüsib autor, millised võimalused on krediidiasutustel isikuandmeid töödelda, lisaks juriidilise kohustuse täitmiseks, ning millisel juhul saab krediidiasutus töödelda isikuandmeid muudel isikuandmete kaitse üldmääruses sätestatud alustel.

Magistritöö kirjutamisel on autor peamiselt tuginenud õigusaktides sätestatule, eriti neljandas rahapesu direktiivis ning isikuandmete kaitse üldmääruses sätestatule. Lisaks kasutas autor töö kirjutamisel erinevate organisatsioonide (nt *Financial Action Task Force*) ning töögruppide (*Working Party 29*) suuniseid ning arvamusi. Kasutatud allikad on suuremas osas Internetipõhised. Magistritöö valmimise ajaks ei ole Euroopa Liidu kohtust veel põhjapanevaid lahendeid ega selgitusi, millises ulatuses ning millist laadi isikuandmeid rahapesu ja terrorismi rahastamise tõkestamiseks rakendavate kohustuse täitmiseks töödelda tuleb, küll on kohtutes ootel eelotsusetaotlused. Seega jääb selle küsimuse vastus tuleviku kohtupraktika kujundada.

Varasemalt on isikuandmete kaitset rahapesu hoolsusmeetmete rakendamisel käsitletud Marleen Jakobsoni magistritöös ''Isikuandmete töötlemise eesmärgipärasuse põhimõte hoolsusmeetmete järgimisel krediidiasutuste poolt''. Siiski on käesoleva magistritöö eesmärk erinev.

Autor loodab, et käesolev magistritöö leiab kasutust krediidiasutustes ning aitab krediidiasutustel leida veelgi parem tasakaal hoolsusmeetmete rakendamise ning isikuandmete töötlemise vahel.

1. RAHAPESU JA TERRORISMI RAHASTAMISE TÕKESTAMISE ÕIGUSAKTIDEST TULENEVAD HOOLSUSMEETMED

Esimeses peatükis analüüsib autor hoolsusmeetmete kohaldamise kohustust, hoolsusmeetmete eesmärki ja hoolsusmeetmete liike. Erinevatest hoolsusmeetmetest ning nende eesmärkidest on oluline aru saada, et edaspidi mõista, mis hoolsusmeetmeid kohaldatakse ning milliseid põhiõigusi hoolsusmeetmete kohaldamisel piirata võidakse.

1.1. Hoolsusmeetmete sisu ja määratletus õigusaktides

Hoolsusmeetmete all on silmas peetud kohustatud isikute, sh krediidiasutuste tegevust rahapesu ning terrorismi rahastamise tõkestamisel. Neljas rahapesu direktiiv sätestab, milliseid toiminguid kohustatud isikud tegema peavad ja millal selliseid toiminguid kohustatud isikud tegema peavad. Direktiiv on Eesti õiguses üle võetud rahapesu ja terrorismi rahastamise tõkestamise seadusesse. Samuti sätestab direktiiv, kui ka RahaPTS kohustatud subjektid, kellele hoolsusmeetmete rakendamise kohustus kohaldub. Kohustatud subjektiks/isikuks on rahapesu neljanda direktiivi artkili 2 lg 1 p 1 ning RahaPTS § 2 lg 1 p 1 kohaselt muuhulgas krediidiasutus. Käesolev magistritöö keskendub krediidiasutustele, mitte muudele isikutele, kes on hoolsusmeetmete rakendamiseks kohustatud.

RahaPTS § 19 lg 1 näeb ette juhud, millal peab kohustatud isik hoolsusmeetmeid rakendama:

a. ärisuhte loomisel;
b. ärisuhte väliselt tehingute juhuti tegemisel või vahendamisel, kui tehingu väärtus on üle 15 000 euro või sellega võrdväärne summa muus vääringud, sõltumata sellest, kas rahaline kohustus täidetakse ühe maksena või mitme maksega, mis on omavahel seotud, kuni üheaastase perioodi jooksul;
c. hoolsusmeetmete kohaldamisel kogutud teabe kontrollimise või asjakohaste andmete ajakohastamise käigus varem kogutud dokumentide või andmete piisavuse või tõelevastavuse kahtluse korral;
d. rahapesu või terrorismi rahastamise kahtluse korral, olenemata ükskõik millisest seaduses nimetatud mööndusest, erandist või piirsummast.

Neljanda rahapesu direktiivi artikkel 14 lg 5 näeb ette, et kohustatud isikud peavad hoolsusmeetmeid kohaldama mitte ainult ärisuhte loomisel, vaid asjakohasel juhul ka olemasolevate klientide suhtes, sealhulgas juhul kui kliendiga seotud asjaolud muutuvad.

Hoolsusmeetmeid peab krediidiasutus kohaldama oma klientide suhtes, kuid enne tuleb krediidiasutusel koostada riskihinnang, mille alusel otsustatakse konkreetse potentsiaalse kliendi puhul, kas temaga ärisuhe luuakse või tehing tehakse. RahaPTS § 13 lg 1 kohustab krediidiasutusi koostama oma tegevusega kaasnevate rahapesu ja terrorismi rahastamisega seotud riskide tuvastamiseks, hindamiseks ja analüüsimiseks riskihinnangu. Siiski ei ole riskipõhine lähenemisviis kohustatud isikute jaoks kõikelubav valikuvõimalus[15]. Riskihinnang hõlmab tõendite alusel otsuste tegemist, et oleks võimalik tõhusamalt suunata kohustatud isikute tegevust rahapesu ja terrorismi rahastamise riskide maandamisele, millega kohustatud isikud silmitsi seisavad[16]. Kohustatud isik peab oma klientide ja enda tegevuses ära tundma rahapesu ja terrorismi rahastamisega seotud riske. Nende riskide analüüsimisel hindab krediidiasutus, milline on tõenäosus riski realiseerumiseks, samuti milline on riski realiseerumise tagajärg[17]. Hinnangu koostamisel tuleb arvesse võtta klientidega seonduvaid riske, näiteks kas klient on riikliku taustaga isik, riikliku taustaga isiku pereliige või lähedane kaastöötaja. Riikliku taustaga isiku puhul on tegemist isikuga, kes teostab avalikku võimu ning nende staatuse ja positsiooni tõttu on risk, et riikliku taustaga isik võib oma positsiooni ära kasutada rahapesu toime panemise eesmärgil, korruptsiooni või terrorismi rahastamise eesmärgil[18]. Lisaks tuleb kohustatud isikul arvesse võtta seda, kas kliendi näol on tegemist mitteresidendiga ning millised riskid seonduvad geograafiliste piirkondade või jurisdiktsioonidega: kas klient pärit kolmandast riigist, mille rahapesu vastased regulatsioonid ei ole samaväärsed EL regulatsioonidega. Lisaks tuleb arvesse võtta toodete, teenuste või tehinguga seonduvaid riske ning kohustatud isiku ja klientide vaheliste suhtlus- või vahenduskanalitega või toodete, teenuste või tehingute edastamiskanalitega seonduv risk. Riskihinnangu tulemusena määrab krediidiasutus kindlaks väiksema või suurema riskiga piirkonnad, riskiisu ulatuse ning riskijuhtimise mudeli, mille hulgas on lihtsustatud ja tugevdatud hoolsusmeetmed tuvastatud riskide maandamiseks.

Kohustatud isiku riskihinnang ei tohi siiski minna vastuollu õigusaktides sätestatuga. On võimalik, et kohustatud isikute riskiisu ja seetõttu ka riskihinnangu tulemused võivad erineda, ehk mõned krediidiasutused on suuremast riskiisust tulenevalt valmis looma ärisuhteid klientidega, kelle puhul on suurem võimalus rahapesu või terrorismi rahastamise alase riski

[15] (EL) 2015/849. Põhjenduspunkt 11
[16] *Ibid.*
[17] Finantsinspektsiooni soovituslik juhend, lk 26, (viide nr 4).
[18] *FATF (Financial Action Task Force*). Guidance. Politically exposed persons (recommendations 12 and 22). 2013. Lk 5. Arvutivõrgus: http://www.fatf-gafi.org/media/fatf/documents/recommendations/guidance-pep-rec12-22.pdf (17.04.2021)

realiseerumine. Siiski ei ole krediidiasutustel võimalik luua ärisuhteid selliste juriidiliste või füüsiliste isikutega, kes on lisatud ametlikesse nimekirjadesse terroristidena[19]. Näiteks oli 2010. aastal USA terroristiorganisatsioonidena üles loetletud 45 organisatsiooni ning selliseid nimekirju koostavad teiste riikide valitsused[20]. Kui krediidiasutus enne ärisuhte loomist tuvastab, et füüsiline või juriidiline isik kuulub mõnda sellisesse nimekirja, ei või krediidiasutus isikuga ärisuhet luua ning juba loodud ärisuhe tuleb lõpetada, välja arvatud, kui erandid on *expressis verbis* sätestatud[21]. Ei ole oluline, millise riigi ametlikus terroristi või terrorismiorganisatsiooni nimekirjas isik on. Kui mõnes Eesti krediidiasutuses soovib arvelduskonto avada isik, kes on näiteks USA valitsuse poolt kehtestatud terroristide või terrorismiorganisatsioonide nimekirjas, kuid ei ole samalaadses nimekirjas näiteks Austraalias, ei tohi Eesti krediidiasutus sellise isikuga ärisuhet luua. Selliste nimekirjade eesmärgiks on teavitada ning hoiatada terroristide või organisatsioonide eest ning kõikide nimekirjas olevate isikute puhul on tõenäoliselt põhjendatud arvata, et need isikud tõepoolest tegutsevad terrorismiga.

Seega tuleb krediidiasutustel täita kindlasti miinimumnõuded hoolsusmeetmete osas, kuid muude riskitegurite hindamisel on antud kohustatud isikutele üsna suur vabadus, milliste klientidega ärisuhteid luua. Siiski ei saa krediidiasutus või muu kohustatud isik õigustada ärisuhte loomist ametlikus nn ''mustas nimekirjas'' oleva isikuga põhjendusega, et kohustatud isiku riskiisu on suurem.

RahaPTS § 42 lg 1 keelab luua ärisuhte isikuga, kelle puhul ei suuda krediidiasutus täita samas seaduses sätestatud hoolsusmeetmeid. Samuti on krediidiasutusel õigus ärisuhe lõpetada, kui klient ei edasta krediidiasutusele hoolsusmeetmete täitmiseks vajalikke tõendeid või muud asjakohast teavet, mida krediidiasutus on küsinud. Sellisel juhul loetakse teabe andmisest keeldumist oluliseks lepingurikkumiseks ning kohustatud isikul on RahaPTS § 42 lg-st 4 kohustus ärisuhe lõpetada. Tähelepanu tasub pöörata asjaolule, et teabe esitamata jätmisel on krediidiasutusel kohustus, mitte õigus, ärisuhe lõpetada. Sellise sõnastusega on seadusandja tõenäoliselt soovinud võtta krediidiasutustelt võimaluse hoida oma kliendiportfellides kliente, kelle ärimudelitest ega omandivormidest pole võimalik vajalikul määral aru saada.

[19] Fratangelo., P. The New Anti-Money Laundering Law. First Perspective on the 4th European Union Directive. Palgrave Macmillan: 2016. Lk 21.
[20] Freedman. B., Officially Blacklisted Extremist/Terrorist (Support) Organizations: a Comparison of Lists form six Countries and two International Organizations. Pespectives on Terrorism. May 2010 vol 4, No 2. Lk 46. Aruvtivõrgus: https://www.jstor.org/stable/pdf/26298448.pdf (21.04.2021).
[21] Fratangelo., P. Lk 21.

Kindlasti tuleb vaidluse korral hinnata, kas teave, mille edastamata jätmisel krediidiasutus ärisuhte kliendiga lõpetab, on siiski asjakohane. On võimalik, et krediidiasutus küsib kliendilt palju teavet, millest osa ei teeni rahapesu või terrorismi rahastamise tõkestamise eesmärki. Sellisel juhul tuleb krediidiasutusel tõendada, et teave, mida küsiti ning mille klient esitamata jättis oli tõepoolest vajalik ning teabe esitamisel oleks krediidiasutusel olnud võimalik kliendisuhet jätkata või see erakorraliselt üles öelda, kuna krediidiasutusel tekkis kahtlus, et tegemist on rahapesu või terrorismi rahastamisega.

RahaPTS § 19 lg 5 järgi tuleb RahaPTS § 20 lg-s 1 p 1-5 sätestatud hoolsusmeetmeid, välja arvatud ärisuhte seire, kohaldada enne ärisuhte loomist või ärisuhte väliselt enne tehingu tegemist. Kohaldatavateks hoolsusmeetmeteks on:

a. kliendi või juhuti tehtavas tehingus osaleva isiku isikusamasuse tuvastamine ning esitatud teabe kontrollimine usaldusväärsest ja sõltumatust allikast hangitud teabe põhjal, sealhulgas e-identimise ja e-tehingute usaldusteenuste vahendite abil;
b. kliendi või juhuti tehtavas tehingus osaleva isiku esindaja isikusamasuse ja esindusõiguse tuvastamine ning kontrollimine;
c. tegeliku kasusaaja tuvastamine ja tema isikusamasuse kontrollimiseks meetmete võtmine ulatuses, mis võimaldab kohustatud isikul veenduda selles, et ta teab, kes on tegelik kasusaaja, ja saab aru kliendi või juhuti tehtavas tehingus osaleva isiku omandi- ja kontrollstruktuurist;
d. ärisuhtest, juhuti tehtavast tehingust või toimingust arusaamine ja asjakohasel juhul selle kohta täiendava teabe kogumine;
e. teabe hankimine asjaolu kohta, kes on riikliku taustaga isik, tema pereliige või tema lähedaseks kaastöötajaks peetav isik;
f. ärisuhte seire.

Isikusamasuse tuvastamiseks tuleb isikul esitada isikut tõendav dokument. Selline isikut tõendav dokument ei saa olla igasugune pildi ning sünnikuupäeva või isikukoodiga dokument (nagu näiteks õpilaspilet). Kohustatud isikud peavad isiku identifitseerimiseks kasutama ametlikke dokumente, mis on väljastatud riigiasutuse poolt[22]. Eestis on sellisteks dokumentideks dokumendid, mis on loetletud isikut tõendavate dokumentide seaduse[23] §-s 2. Täiendavalt võib krediidiasutus saadud teavet kontrollida näiteks Politsei- ja Piirivalveametile päringuid tehes või nende andmebaasist. Kuna Politsei- ja Piirivalveamet väljastab isikut

[22] Basel Committee on Banking Supervision. Customer due dilligence for banks. October 2001, lk 20.
[23] RT I, 31.01.2020, 15.

tõendavaid dokumente Eesti Vabariigis, on tegemist piisavalt usaldusväärse ning sõltumatu allikaga. Kui ärisuhet soovitakse luua isikuga, kes ei ole Eesti Vabariigi kodanik, resident ning esitatakse välismaine dokument, tuleks autori arvates nõuda, et isik esitaks oma dokumendi originaali või koopia, mille õigsus on välisriigi pädeva asutuse poolt tõestatud või kinnitatud. Niimoodi on võimalik kohustatud isikul veenduda dokumendi õigsuses, kuna seda, kas pädev asutus on sellist dokumenti tõestanud või kinnitanud, on võimalik samalt pädevalt asutuselt teada saada. Välisriigis välja antud dokumentide puhul notariaalse kinnitamise või tõestamise nõue on sätestatud näiteks Inbank AS üldtingimustes[24]. Samuti tuleks autori arvates nõuda, et selline dokument ei tohiks olla liiga vana. Vastasel juhul ei pruugi esitatud teave olla enam ajakohane. Näiteks kui juriidilise isiku puhul esitab juhatuse liige registrikaardi väljavõtte, mis on kaks aastat vana, ei saa seda pidada ajakohaseks, kuna juhatuse liikme volitused võivad olla lõppenud, kuid seda ei nähtu esitatud registrikaardi väljavõttelt. Selline ajaperiood peaks olema kehtestatud kohustatud isiku sisereeglites ja sellise ajaperioodi pikkus sõltub kohustatud isiku riskiisust ning -hinnangust.

Esindusõiguse kontrollimiseks tuleb kontrollida esitatud volikirja. Tihti võivad esitatavad volikirjad olla välismaised, mistõttu tuleb eriti hoolikalt kontrollida nende õigsust, ehk kas volikiri on legaliseeritud[25] või varustatud *apostille*'ga[26]. Eestis väljastatud notariaalse volikirja puhul võib krediidiasutus ühendust võtta volikirja tõestanud notariga, kes kinnitaks volikirja õigsust. Füüsilise isiku tuvastamisel tuleb tuvastada ka füüsilise isiku tegelik kasusaaja, ehk isiku tegevust kontrolliv ja sellest kasu saav isik. Seda tuleb kontrollida eelkõige, kui hoolsusmeetmete rakendamisel tekib kahtlus, et füüsilist isikut on kallutatud tehingu tegemisele. Sellisel juhul on tegelik kasusaaja isik, kes teostab füüsilise isiku üle, kes tehingut teostab, kontrolli[27]. Selline olukord võib tekkida näiteks siis, kui krediidiasutuse kontoris soovib arvelduskontot avada või laenu võtta isik, kelle puhul tekib kahtlus, et ta ei tee neid toiminguid oma tarbeks. Sellisele tegutsemisele võib viidata olukord, kus teenust sooviva isikuga on kaasas teine isik, kes ise pigem vastab küsimustele või ei soovita teenust soovival isikul täiendavatele küsimustele vastata. Sellisel juhul tuleks eeldada, et krediidiasutuse kontoris viibiv isik ei soovi neid teenuseid kasutada enda tarbeks, vaid neid teenuseid hakkab kasutama keegi teine muudel eesmärkidel. Sellises olukorras ei peaks krediidiasutuse töötaja

[24] Inbank AS üldtingimused. P 7.2. Arvutivõrgus: https://www.inbank.ee/documents/ee/et/pdf/general_conditions_3.pdf (13.04.2021).
[25] Legaliseerimine on formaalsus, millega välisriigi pädev ametiasutus kinnitab avaliku dokumendi allkirja ja dokumendil oleva pitseri või templi ehtsust või allakirjutanud isiku pädevust.
[26] *Apostille* on tunnistus, millega kinnitatakse dokumendile alla kirjutanud isiku pädevus.
[27] Finantsinspektsiooni juhend (viide nr 4), lk 34.

pakkuma isikule soovitavat teenust, vaid küsima täiendavat teavet. Teabe esitamata jätmisel ei ole lubatud krediidiasutusel ärisuhet luua.

Juriidilisest isikust kliendi puhul tuleb samuti tuvastada isikusamasus. Kuna juriidiline isik tegutseb füüsiliste isikute kaudu, tuleb tuvastada juriidilise isiku esindajad nii, nagu tuleb tuvastada isikusamasus füüsilise isiku puhul. Viies rahapesu direktiiv[28] lisas kohustuse äriühinguga kliendisuhte loomisel isikusamasuse tuvastamisel esitada registreerimistõend või registri väljavõte, kui äriühingu tegelik kasusaaja on vaja registreerida. Eesti krediidiasutuste puhul tähendaks see seda, et enne äriühinguga kliendisuhte loomist tuleb krediidiasutusele esitada äriregistri väljavõte, kust nähtub äriühingu tegelik kasusaaja. See ei tähenda, et äriühing peab dokumendid esitama paberkandjal. Selleks võib esitada näiteks pdf faili kujul väljavõtte äriregistrist (tõenäoliselt oleks aktsepteeritav registri kuvatõmmis, kust kasusaaja nähtub). Oluline on see, et äriühing esitaks väljavõtte registrist ning krediidiasutusel oleks võimalik kontrollida, kas äriühingu poolt esitatav teave on korrektne.

Tegeliku kasusaaja tuvastamine on autori arvates kõige olulisem hoolsusmeede, mida ärisuhte loomisel kohaldada tuleb. Vastasel juhul võib märkamata jääda, kelle huvides tegelikult ärisuhe luuakse või tehing viiakse lõpule seetõttu, et formaalselt teeb tehingu isik, kelle suhtes ei teki krediidiasutusel kahtlust, et kliendi puhul võib olla seotus rahapesu või terrorismi rahastamisega.

Rahapesu neljanda direktiivi artiklid 30 ning 31 reguleerivad tegeliku kasusaaja tuvastamise kohustust. Artikkel 30 lg 1 sätestab, et liikmesriigid tagavad, et nende territooriumil registreeritud äriühingud või muud õiguslikud üksused peavad koguma ja hoidma asjakohast, täpset ja ajakohastatud teavet oma tegelikult kasu saavate omanike kohta, mis hõlmab ka kasu saamisega seotud üksikasju. Viies rahapesu direktiiv lisab sinna juurde kohustuse liikmesriikidele tagada, et tegelike kasusaajate kohta teabe kogumise kohustuse rikkumise korral kohaldatakse tõhusaid, proportsionaalseid ja hoiatavaid meetmeid ja karistusi. Eestis tuleb eraõigusliku juriidilise isiku tegeliku kasusaaja andmeid RahaPTS § 76 lg 1 kohaselt hoida äriregistri juures. Autori arvates ei pruugi Eesti krediidiasutuste puhul olla piisav tegevus kontrollida Eestis registreeritud eraõigusliku juriidilise isiku tegelikku kasusaajat äriregistrist,

[28] Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2018/843, millega muudetakse direktiivi (EL) 2015/849, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist, ning millega muudetakse direktiive 2009/138/EÜ ja 2013/36/EL (viies rahapesu direktiiv) – ELT L 156. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32018L0843&from=EN

kuna äriseadustiku (ÄS)[29] § 34 ning Riigikohtu selgituste[30] järgi on äriregistri kannetel deklaratiivne tähendus, välja arvatud kannetel, mille konstitutiivne tähendus tuleneb üheselt seadusest. RahaPTS §-st 76 ei nähtu, et tegelike kasusaajate kannetel oleks omistatud õiguslik tähendus, mistõttu kehtib ÄS § 34 lg-st 2 tulenev registrikande avaliku usaldatavuse põhimõte ehk kanne kehtib kolmanda isiku suhtes õigena, välja arvatud siis, kui kolmas isik teab või pidi teadma, et see kanne on väär. Seetõttu peaksid autori arvates krediidiasutused küsima lisateavet tegelikult kasu saavate isikute kohta ning seda teavet saaks näiteks võrrelda äriregistris oleva teabega. Kui äriühingu poolt esitatud tegeliku kasusaaja andmed ei kattu äriregistris avaldatuga, tuleb krediidiasutusel küsida täiendavat teavet. Kui teavet ei esitata või esitatakse ebapiisav teave, mille puhul tekib krediidiasutusel kahtlus, et tegemist võib olla rahapesu või terrorismi rahastamisega, ei ole lubatud sellise isikuga ärisuhet luua või juba loodud ärisuhe tuleb lõpetada (RahaPTS § 42 lg 1, 4).

Tegeliku kasusaaja tuvastamine võib osutuda keeruliseks, kui äriühingul, kellega soovitakse kliendisuhet luua, on väga keeruline omandistruktuur ning selles struktuuris ei nähtu ühtegi füüsilist isikut, kes võiks olla tegelik kasusaaja. Näiteks osaühing A, mille osanikeks on osaühing B (20%), osaühing C (40%) ning osaühing D (40%). Osaühingud B, C ning D osanikud on samuti äriühingud ning sellisest struktuurist ei nähtu osanike seas ühtegi füüsilist isikut, vaid kõik äriühingud on omatud teiste äriühingute poolt. Eriti keeruline on struktuur siis, kui kuskilt maalt omab äriühingut selline äriühing, mis on registreeritud välisriigis ning sellise välisriigi õiguse järgi ei ole vaja tuvastada kasusaajat füüsilise isiku tasandil. See võib juhtuda siis, kui äriühingu omanik ei ole Euroopa Liidus registreeritud. Niivõrd keeruka omandistruktuuri puhul võib tegemist olla skeemiga, kus üritataksegi tegelikku kasusaajat varjata erinevate äriühingute kaudu, kuid pole välistatud, et suuremate äriühingute omandistruktuur võibki niivõrd keeruline ja mitmetasandiline olla. Seega tuleb krediidiasutustel selliste keeruliste omandistruktuuride puhul olla ettevaatlik ning küsida lisateavet nii kaua kuniks leitakse füüsiline isik, kes on tegelik kasusaaja. Vastasel juhul võib juhtuda, et asutakse tehinguid tegema kahtlaste isikutega ning krediidiasutust võib järelevalve selle eest rahaliselt trahvida.

Kuigi neljas rahapesu direktiiv ja RahaPTS (§ 9) sätestab, et tegelikult kasu saaval isikul peaks olema vähemalt 25% pluss üks aktsia või 25% osalusest, ei pruugi ole kontroll osaluse kaudu

[29] RT I, 04.01.2021, 46
[30] RKHKm 3-19-1672, p 20.

alati tuvastatav. On võimalik, et äriühingus on füüsilisel isikul osanike kokkuleppe järgi valitsev mõju, isegi kui see isik ei oma seadusest tulenevat 25% suurust osalust.[31]

Kui krediidiasutusel ei õnnestu tuvastada selliseid füüsilisi isikuid, kes vastaksid eeltoodud kriteeriumitele, saab RahaPTS § 9 lg 4 järgi tegelikult kasu saavaks isikuks lugeda sellist füüsilist isikut, kes on kõrgema juhtorgani liige. Seda võimalust kasutatakse juhtudel, kui on ammendunud kõikvõimalikud tuvastusmeetodid ja ikkagi pole õnnestunud kindlaks teha tegelikku kasusaajat ja puudub kahtlus, et tegelik kasusaaja siiski eksisteerib. Sellist võimalust võidakse kasutada ka siis, kui on kahtlus, kas kindlaks tehtud isik ikkagi on tegelik kasusaaja. Seega kui tegelik kasusaaja on oma seost juriidilise isiku ja selle varadega niivõrd hästi varjanud, peetakse tema asemel tegelikuks kasusaajaks mõnda juhtorgani liiget. RahaPTS § 9 lg 4 on üle võetud neljandast rahapesu direktiivist, mille artikli 3 p 6 alapunkti a (ii) järgi hõlmab ''tegelikult kasu saava omaniku'' mõiste ka füüsilist isikut või isikuid, kes on kõrgema juhtkonna liikmed ja kui ei ole võimalik enam tuvastada tegelikku kasusaajat. Selline olukord võib tekkida äriühingus, mille aktsiaosalus on niivõrd hajutatud ja seetõttu on võimatu osutada kasusaavale omanikule.[32] RahaPTS § 29 järgi rakendatakse kõiki hoolsusmeetmeid, sh tegeliku kasusaaja tuvastamist mittetulundusühingute ning sihtasutuste suhtes.

Eeltoodust nähtub, et keerukate äriühingute omandistruktuuride taha soovivad end peita sellised isikud, kellega oleks muidu keelatud tehinguid teha või ärisuhet luua. Seetõttu on autori hinnangul krediidiasutustel seega väga oluline kohustus teada saada, kes on see konkreetne füüsiline isik või isikud, kes saavad kasu loodavast ärisuhtest või tehingust.

Ärisuhte või juhuti tehtava tehingu puhul peab krediidiasutus aru saama tehingu eesmärgist ning selle olemusest. Ärisuhtest aru saamine on oluline, kuna võimaldab krediidiasutusel kergemini märgata ebaharilikke tehinguid, või tehinguid, mis on tavapärasest oluliselt suurema väärtusega. Selliste olukordade puhul on asjakohane ning vajalik koguda täiendavat teavet. Selliseks täiendavaks teabeks võib olla kliendi või juhuti tehtava tehingu puhul tehingupoolte püsiva tegevusala, maksutavade, olulisemate tehingupartnerite kohta informatsiooni kogumine. Samuti on ärisuhte või juhuti tehtava tehingu eesmärgist arusaamine oluline, kuna aitab välja selgitada, kas pakutav teenus vastab kliendi tegelikule finantsteenuse soovile. Kliendi

[31] Rahandusministeeriumi juhend. Juhis tegeliku kasusaaja määratlemiseks. Rahandusministeerium. Lk 2. Arvutivõrgus: https://www.rahandusministeerium.ee/sites/default/files/tegelike_kasusaajate_andmete_esitamise_juhis_.pdf (21.02.2021)

[32] Tibar, I. Tähelepanekuid uue rahapesu ja terrorismi rahastamise tõkestamise seaduse jõustumisega seoses. – Juridica 2018/I, lk 45.

maksetavad ja tema tegevusvaldkond ja äripartnerid peaksid olema iseloomulikud turule, milles klient tegeleb. Vastasel juhul võib tekkida kahtlus tegeliku kasusaaja isikus. Kui juriidilisest isikust klient soovib ühtäkki täiesti teistsugust finantsteenust, mida ei ole konkreetne juriidiline isik kunagi kasutanud ega kasuta reeglina teised samas valdkonnas tegutsevad juriidilised isikud, võib ja peaks selline tegevus tekitama krediidiasutuses kahtlust ka selle osas, kelle huvides uut finantsteenust tegelikult soetada soovitakse.

Maksetavade puhul tuleb välja selgitada, milliseid ning millises koguses klient finantsteenuseid tarbib. Arvelduskonto puhul tuleb jälgida kuus või aastas tehtavaid tehinguid ja nende kogust. Samuti nende tehingute sihtriigid või millistest riikidest äripartneritelt maksed laekuvad. Lisaks, kui klient tegutseb väärtpaberiturul: väärtpaberite ostmise, müümise sagedus, väärtpaberite realiseerimisega kaasnev hulk jms.[33] Täiendava teabe kogumiseks võib krediidiasutus tehtava tehingu RahaPTS § 43 lg 1 alusel edasi lükata.

Ärisuhte seire on ärisuhte kestel kliendi tegevuse monitoorimine. Seega ei ole ärisuhte seire ühekordne hoolsusmeede, vaid kestev. Selle eesmärgiks on see, et klienti ei tuvastataks vaid ühe korra ja hoolsusmeetmeid kohaldataks vaid enne ärisuhte loomist ja edaspidi saab klient teha kahtlaseid tehinguid. Ärisuhte seire aitab autori hinnangul kõige paremini tuvastada kliendiga seotud riske ärisuhte ajal. Ärisuhte seire hõlmab endas klientide maksekäitumise pidevat jälgimist, mistõttu peaks mõni tavapärasest suurem tehingusumma või tavapärasest tihedamad tehingud andma märku, et kliendi käitumine on muutunud ning sellisel juhul saab kohaldada juba täiendavaid hoolsumeetmeid ja nõuda kliendilt täiendavat teavet kahtlust tekitavate tehingute kohta.

Kõiki hoolsusmeetmete käigus kogutud andmeid (sealhulgas isikuandmeid) tuleb krediidiasutustel säilitada, et tagada koostöö järelevalveasutustega. Kohustatud isik on kohustatud registreerima tehingu tegemise kuupäeva või ajavahemiku ning tehingu sisu ja kirjelduse (RahaPTS § 46 lg 1). Samuti on krediidiasutusel kohustus registreerida RahaPTS § 46 lg-tes 2-3 sätestatud teave. RahaPTS § 47 kohaselt tuleb isikusamasuse tuvastamiseks kogutud dokumentide originaale või koopiad, ärisuhte loomise aluseks olevaid dokumente ning RahaPTS § 46 järgi registreeritud teavet, säilitada viis aastat pärast ärisuhte lõppemist.

[33] Finantsinspektsiooni juhend (viide nr 4). lk 45-47.

Autori arvates võib viieaastane andmete säilitamise aeg olla liiga lühike, kuivõrd rahapesu ja terrorismi rahastamise tõkestamise reeglite rikkumine võib ilmsiks tulla pärast viit aastat ärisuhte lõpetamist. Näiteks on Finantsinspektsioon oma 18.03.2020 juhatuse otsuses, millega tehti ettekirjutus Swedbank AS-le selgitanud, et rahapesu hoolsusmeetmete rikkumine on toimunud alates aastast 2007[34]. Danske panga kaasuses oli samuti rikkumisi toime pandud alates aastast 2007[35]. Viidatud kaasustest nähtub, et rikkumised avastatakse palju hiljem ning kui kohustatud isik säilitab andmeid seadusest tulenevalt viis aastat, on hiljem keeruline, kui mitte võimatu tuvastada varasemaid rikkumisi. Siiski, kuna hoolsusmeetmete käigus kogutakse muuhulgas isikuandmeid, tuleb autori hinnangul arvestada isikuandmete kaitse õigusega, mille üheks osaks on isiku õigus olla unustatud[36]. Seega ei pruugi isikuandmete kaitse perspektiivist põhjendatud ja õiglane säilitada isikuandmeid kauem kui viis aastat. On arusaadav, et uurimisasutuste jaoks on pikema andmete säilitamise aja korral tõenäolisem rikkumiste tuvastamine, kuid õigust isikuandmete kaitsele ei tohiks autori hinnangul piirata vaid seetõttu, et uurimisasutused ei ole võimelised viie aastase perioodi jooksul rikkumisi tuvastama. Andmed, mida isikutelt kogutakse AS SEB pangas arvelduskonto avamisel on näiteks nimi, isikukood ja sünniaeg, mis on saadavad isiku isikutunnistuselt. Samuti peab isik tõendama seose Eestiga, näiteks elamine Eestis, mis tähendab, et kogutakse teavet isiku asukoha kohta[37]. Euroopa Liidu Kohus on selgitanud, et andmed, mida säilitavad elektroonilise side teenuste osutajad (nt mh registreeritud kasutaja aadress), koosvõetuna võimaldavad teha väga täpseid järeldusi andmesubjektide eraelu kohta[38]. Sellist andmete kogumist ning töötlemist on kohus pidanud eriti raskeks isikuandmete kaitse õiguse riiveks. Kui krediidiasutuse andmelekke tagajärjel peaks avalikult kättesaadavaks saama klientide nimed, isikukoodid, sünniajad ning elukoha aadress, on nende andmete pinnalt ja koosmõjus võimalik teha järeldusi isiku eraelu osas ning seetõttu riivab selliste andmete töötlemine autori hinnangul isiku õigust oma andmete kaitsele raskelt. Sellisel juhul peab olema väga kaalukas põhjus, miks andmeid sellises mahus töödeldakse, milleks rahapesu hoolsusmeetmete rakendamisel on finantssektori läbipaistvuse tagamine ning ebaseaduslike rahavoogude ringlusesse sattumise takistamine. Autori arvates oleks võinud seadusandja jätta kohustatud isikutele kaalutlusruumi, et väga väikese riskiga klientide andmed võidaks kustutada enne viie aasta möödumist. Sellise sättega oleks tõenäoliselt kaasnenud oht, et kohustatud isikud kipuvad andmeid kustutama enne viie aasta

[34] Finantsinspektsiooni 18.03.2020 juhatuse otsus nr 4.1-1/40 ''Ettekirjutus Swedbank AS-le nõudmises viia oma tegevus kooskõlla krediidiasutuste tegevust reguleerivate õigusaktidega'', lk 6.
[35] Finantsinspektsiooni 19.02.2019 juhatuse otsus (viide 1). lk 5.
[36] Õigus olla unustatud tuleneb isikuandmete kaitse üldmääruse (EL) 2016/679 artiklist 17.
[37] Teave AS SEB panga arvelduskonto avamisest: https://www.seb.ee/igapaevapangandus/kontod-ja-arveldused/arvelduskonto (12.04.2021).
[38] EKo C-203/15, *Tele2 Sverige AB vs Post-och teletyrelsen.* ECLI:EU:C:2016:970. p 98.

möödumist põhjendusega, et nende hinnangul ei kuulunud konkreetne klient riskirühma ning võivad sellise käitumisega takistada süütegude avastamist. Seega oleks seadusandja pidanud andma ka tegurid, mida arvesse võtta, kui otsustada, kas kliendiandmed enne viit aastat pärast kliendisuhte lõppemist kustutada.

Andmete säilitamise kohustus hõlmab ka ärisuhte seire ning selle ajal hoolsusmeetmete kohaldamisega seotud kirjavahetuse ning muude dokumentide säilitamist. Lisaks tuleb säilitada juhuti tehtavate tehingute käigus kogutud andmed ja dokumendid, sealhulgas andmed kahtlaste või ebatavaliste tehingute või asjaolude kohta, millest krediidiasutus Rahapesu Andmebürood ei teavitanud (RahaPTS § 47 lg 2). Kui krediidiasutus täidab RahaPTS § 49 alusel teavitamiskohustust, tuleb ka teavitamiskohustuse aluseks olevaid dokumente RahaPTS § 47 lg 3 järgi säilitada viis aastat pärast tehingu tegemist või teavituskohustuse täitmist. Sama sätte neljanda lõike järgi tuleb krediidiasutusel säilitada eelnimetatud dokumente sellisel viisil, mis võimaldab dokumendid viivitamatult edastada Rahapesu Andmebüroole, teistele järelevalveasutustele, uurimisorganitele või kohtule. Kuivõrd seadus ei sätesta täpsemalt andmete säilitamise viisi, võib andmeid säilitada nii paberkandjal, kui ka elektroonilistes andmebaasides. Viimase puhul on niivõrd mahukate andmete säilitamine ilmselt lihtsam, samuti on elektrooniliselt andmeid säilitades neid lihtsam pädeva asutuse päringu korral edastada.

1.2. Hoolsusmeetmete liigid ja nende kohaldamine

Erinevate hoolsusmeetmete sisu mõistmise kaudu on võimalik aru saada, milliseid isikuandmeid ja millisel hulgal erinevatel juhtudel krediidiasutused koguvad. Käesolevas alapeatükis kirjeldab autor erinevaid hoolsusmeetmete liike ning nende kohaldamise vajadust erinevates olukordades. Neljas rahapesu direktiiv ja RahaPTS näevad ette kolme liiki hoolsusmeetmeid: üldised, lihtsustatud ning tugevdatud hoolsusmeetmed. Üldiste hoolsusmeetmete sisu on autor analüüsinud eelnevas alapeatükis. Seetõttu analüüsib autor käesolevas alapeatükis vaid lihtsustatud ning tugevdatud hoolsusmeetmete sisu ning nende kohaldamise juhtusid. Hoolsusmeetmete sisust ning nende rakendamise käigus kogutavate isikuandmete mahust on autori hinnangul oluline aru saada, kuna see aitab mõista kas ja millisel määral piiratakse isikute õigusi isikuandmete kaitsele.

1.2.1. Lihtsustatud hoolsusmeetmed

Neljanda rahapesu direktiivi artikkel 15 lg 1 näeb ette, et kui liikmesriik või kohustatud isik teeb kindlaks väiksema riskiga valdkonnad, võib kõnelaune liikmesriik lubada kohustatud isikutel rakendada kliendi suhtes lihtsustatud hoolsusmeetmeid. Kliendi suhtes lihtsustatud hoolsusmeetmete kohaldamine tähendab hoolsusmeetmete kohaldamist kliendisuhte loomisel, kliendi teostatud tehingu osas ärisuhte kestel või juhuti tehtava tehingu puhul[39].

Väiksema riskiga valdkonnad, millal võib kohustatud isik lihtsustatud hoolsusmeetmeid kohaldada, tuvastatakse riskianalüüsi teostamisel. Riskide hindamisel võivad liikmesriigid ja kohustatud isikud neljanda rahapesu direktiivi artikli 16 kohaselt arvesse võtta vähemalt lisas II loetletud väiksemat riski iseloomustavaid tegureid. Lisas II loetletud väiksemat riski iseloomustsvad tegurid on:

1) Kliendi isikuga seotud riskid:
   a. börsil noteerid äriühingud, kelle suhtes kohaldatakse avalikustamiskohustusi (tuginedes börsieeskirjadele või seadusele või maksmapaneku viisidele), millega on kehtestatud nõuded, et tagada tegelikult kasu saava omaniku piisav läbipaistvus;
   b. ametiasutused või riigiettevõtted;
   c. kliendid, kes on geograafilise riskiteguri tõttu väiksema riskiga geograafiliste piirkondade residendid.
2) Toote, teenuse, tehingu või edastamiskanaliga seotud riskitegurid:
   a. väikse kindlustusmaksega elukindlustuslepingud;
   b. pensioniskeemide kindlustuslepingud, kui need ei sisalda ennetähtaegse tagasiostmise valikuõigust ning neid ei saa kasutada tagatisena;
   c. töötajate väljateenitud aastate pensioni või muid sarnaseid pensionihüvitisi võimaldav skeem, mille puhul kindlustusmaksed arvatakse palgast maha ning pensioniskeemi tingimused ei võimalda skeemis osaleja huvide ülekandmist;
   d. finantstooted või -teenused, mis pakuvad asjakohaselt kindlaksmääratud ja piiratud teenuseid teatavatele kliendirühmadele, et suurendada juurdepääsu finantsalase kaasamise eesmärgil;
   e. tooted, mille puhul rahapesu ja terrorismi rahastamise riski juhitakse muude teguritega nagu raha pealelaadimise piirangud või omandi läbipaistvus (nt teatavat liiki e-raha).
3) Geograafilised riskitegurid:

[39] Finantsinspektsiooni juhend (viide nr 4). Lk 56.

a. liikmesriigid;
b. kolmandad riigid, kellel on rahapesu ja terrorismi rahastamise tõkestamise tõhusad süsteemid;
c. kolmandad riigid, kus usaldusväärsete allikate kohaselt on korruptsiooni või muu kuritegeliku tegevuse tase madal;
d. kolmandad riigid, kus usaldusväärsete allikate, nagu vastastikuse hindamiste, üksikasjaliku hindamise aruannete või avaldatud järelaruannete kohaselt on kehtestatud rahapesu ja terrorismi rahastamise tõkestamise nõuded, mis on kooskõlas FATFi[40] muudetud soovitustega, ning kes neid nõudeid tõhusalt rakendavad.

Eelnevast nähtub, et klientidega seotud riskide puhul tuleb arvesse võtta eelkõige seda, kui läbipaistev ning arusaadav on kliendi tegevus. Samuti on börsil noteeritud äriühingute, ametiasutuste või riigiettevõtete puhul võimalik teavet saada avalikest ning usaldusväärsetest allikatest. Seetõttu puudub vajadus sellistelt klientidelt tihti teavet küsida.

Geograafiliste riskitegurite puhul on iseenesest mõistetav, et kliendid, kes on registreeritud (juriidiliste isikute puhul) või resideeruvad Euroopa Liidu liikmesriigis, on väiksema riskiga kliendid, kuna kõikides Euroopa Liidu liikmesriikides on kohustus rahapesu ja terrorismi rahastamise vastased õigusaktid siseriiklikusse õigusesse üle viia. Kuna kolmandatel riikidel pole kohustust Euroopa Liidu õigusakte enda õigusesse üle võtta, võib olla keeruline otsustada, kas kolmandast riigist pärit kliendiga on mõistlik ja võimalik kliendisuhe luua. Selleks on FATF koostanud nimekirja kõrge riskiga riikidest. Selles nimekirjas olevate riikide kodanike, äriühingute ning residentidega tehingute tegemine ei ole keelatud, kuid neis riikides ei ole kasutusele võetud piisavaid meetmeid rahapesu ja terrorismi rahastamise vastaseks võitluseks. 2021 aasta veebruari seisuga oli FATF kõrge riskiga riikide nimekirjas 19 riiki[41]. See ei tähenda, et kõik riigid, kes FATF kõrge riskiga riikide seas ei ole, on riigid, mille kuritegevuse või korruptsiooni tase on piisavalt madal, et nende kodanike, äriühingute või residentide korral kohaldada lihtsustatud hoolsusmeetmeid. Seega tuleb igal krediidiasutusel koostada enda riskiisust ning riskihinnangust tulenevalt nimekiri riikidest, mille residentide, kodanike või äriühingutega tehinguid üldse ei tehta või kohaldatakse hoopis tugevdatud hoolsusmeetmeid. Olenevalt krediidiasutuse riskiisust, võivad need krediidiasutuste sisesed nimekirjad erineda.

[40] FATF (*Financial Action Task Force)* on 1989 aastal loodud valitsustevaheline organisatsioon, mille eesmärk on välja töötada poliitikaid rahapesu ja terrorismi rahastamise tõkestamisel.
[41] Jurisdictions under Increased Monitoring – February 2021. Arvutivõrgus: http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-february-2021.html (29.02.2021).

Näiteks võib üks krediidiasutus otsustada, et teatud riigi kodanike või äriühingutega kliendisuhete loomine on lubatav, teine krediidiasutus aga keelab oma töötajatel sama riigi äriühingute või kodanikega tehinguid tegemast või ärisuhteid loomast.

RahaPTS täiendab neljanda rahapesu direktiivi lisas II toodud riske vähendava kliendiga seotud asjaolusid. Eesti seadusandja on pidanud kliendiga seotud riski maandavaks asjaoluks muuhulgas seda, kui avalik – õiguslik juriidiline isik on registreeritud Eestis. Autori arvates on seadusandja teadlikult lisanud riski maandava asjaoluna avalik – õigusliku juriidilise isiku, mitte eraõigusliku juriidilise isiku. Olenemata sellest, et eraõiguslik juriidiline isik on Eestis registreeritud, võib sellise eraõigusliku juriidilise isiku tegevus peamiselt toimuda väljaspool Eestit. Seetõttu on krediidiasutustel siiski vajalik monitoorida selliste äriühingute tehinguid ning maksekäitumist ja kahtluse puhul tuleb kindlasti kohaldada täiendavaid hoolsusmeetmeid. Seega ei oleks autori arvates asjaolu, et eraõiguslik isik on registreeritud Eestis, riski maandav, et sellise kliendi puhul oleks õigustatud kohaldada lihtsustatud hoolsusmeetmeid.

Lihtsustatud hoolsusmeetmete kohaldamisel tuleb siiski kohaldada üldisi hoolsusmeetmeid (isikute tuvastamine, kasusaajate tuvastamine, tehingutest arusaamine, ärisuhte seire).

Näiteks võib lihtsustatud hoolsusmeetmete kohaldamisel tuvastada isikusamasuse ja tegeliku kasusaaja pärast ärisuhte loomist või vähendada isikusamasuse tuvastamise tihedust ärisuhte ajal. Samuti võib lihtsustatud hoolsusmeetmete kohaldamisel vähendada pidevat rahavoogude ning tehingute monitoorimist, kuid arvestada tuleb rahavoo suurust ning ei pea kliendilt koguma niivõrd detailseid andmeid tehingutest arusaamiseks või arusaamiseks ärisuhte olemusest, kui neid saab eeldada tehingu tüübist. [42]

RahaPTS on lihtsustatud hoolsusmeetmete kohaldamise jaoks andnud Eesti krediidiasutustele täpsemad juhised ning nõuded, millal võib lihtsustatud hoolsusmeetmeid kohaldada. Nimelt peab RahaPTS § 33 lg 3 järgi olema sõlmitud kliendiga kirjalikus, elektroonilises või kirjalikku taasesitamist võimaldavas vormis kestvusleping või kohustatud isikule laekuvad maksed ärisuhte raames ainult konto kaudu, mida asub Eesti krediidiasutuses või välismaal registreeritud krediidiasutuses, millel on filiaal Eestis, kuid ise on registreeritud Euroopa Majanduspiirkonnas. Samuti peab tehingute sissetulevate ja väljaminevate maksetele olema

[42] International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations. Updated October 2020 (FATF suunised). lk 70. Arvutivõrgus: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf (21.04.2021).

seatud piirmäär. Finantsinspektsioon on oma juhendis selliseks tehingute sissetulevate ja väljaminevate maksete piirmääraks seadnud 15 000 eurot[43].

Siiski tuleb lihtsustatud hoolsusmeetmete kohaldamisel tegeleda klientide ja nende tehingute pideva monitoorimisega. Asjaolu, et krediidiasutus on esialgse riskianalüüsi tulemusena leidnud, et kliendi suhtes võib rakendada lihtsustatud hoolsusmeetmeid, ei tähenda seda, et kliendi tegevus terve ärisuhte ajal on piisavalt väikese riskiga. Kui krediidiasutus avastab sellise kliendi osas ebatavalisi tehinguid, muutusi maksekäitumises või tehingupartnerites, tuleb kindlasti kohaldada täiendavaid hoolsusmeetmeid. Kindlasti ei või kohaldada lihtsustatud hoolsusmeetmeid, kui kohustatud isikul tekib rahapesu või terrorismi rahastamise kahtlus. Seega peavad kohustatud isikud olema igal hetkel valmis vaatama üle klientide suhtes kohaldatavad hoolsusmeetmed ning neid muutma ja vajadusel küsima kliendilt rohkem teavet. Kui klient ei vasta sellesisulisele teabenõudele, kohaldub RahaPTS § 42 lg 4 ning krediidiasutusel on õigus ärisuhe erakorraliselt lõpetada.

Neljas rahapesu direktiiv ega RahaPTS ei näe lihtsustatud hoolsusmeetmete kohaldamisel andmete säilitamise tähtaja osas erandit. See tähendab, et lihtsustatud hoolsusmeetmete kohaldamisel, sarnaselt üldiste hoolsusmeetmetega, peab kohustatud isik säilitama isikusamasuse tuvastamise ja esitatud teave kontrollimise aluseks olevate dokumentide originaale või koopiad viis aastat pärast ärisuhte lõppemist. Sama kaua tuleb säilitada dokumente, mis on olnud muude hoolsusmeetmete rakendamisel (sh juriidilise isiku isikusamasuse tuvastamisel ja juriidilisest isikust kliendi kohta andmete kogumisel ning ärisuhte seire aluseks olevad dokumendid) kogutud (RahaPTS § 47 lg 1).

Lihtsustatud hoolsusmeetmete kohaldamiseks on krediidiasutusel vaja koguda sama laadi isikuandmeid nagu üldiste hoolsusmeetmete korral, kuid kogutav andmete maht võib olla väiksem, kui üldiste hoolsusmeetmete kohaldamisel. FATF suuniste järgi võib näiteks vähendada toimingute monitoorimise tihedust ning harvem uuendada klientide andmeid.

1.2.2 Tugevdatud hoolsusmeetmed

Teatud klientide suhtes tuleb krediidiasutustel ning muudel kohustatud isikutel kohaldada tugevdatud hoolsusmeetmeid. Tugevdatud hoolsusmeetmete kohaldamine eeldab seda, et

[43] Finantsinspektsiooni juhend (viide nr 4). Lk 57.

kliendi isikuga, kliendi päritoluga (geograafiliselt) või tootega seotud risk on keskmisest suurem, mistõttu on vaja koguda rohkem teavet klientide, nende tehingupartnerite ja maksekäitumise kohta, samuti jälgida selliste klientide tegevust, et kiirelt märgata kahtlasi tehinguid. Seega tähendab tugevdatud hoolsusmeetmete kohaldamine seda, et krediidiasutus kohaldab tavapärastele kohustuslikele hoolsusmeetmetele midagi lisaks[44].

Kliendi suhtes tugevdatud hoolsusmeetmete kohaldamist reguleerib neljandas rahapesu direktiivis kolmas jagu (art-d 18-24). Lisaks täiendab tugevdatud hoolsusmeetmete kohaldamise jagu viies rahapesu direktiiv.

Neljanda rahapesu direktiivi art 18 lg 1 sätestab, et artiklites 19 – 24 osutatud juhtudel ning kui tegeletakse komisjoni poolt kindlaks määratud suure riskiga kolmandates riikides[45] tegutsevate füüsiliste isikute või nendes riikides asutatud juriidiliste isikutega, samuti muudel liikmesriikide või kohustatud isikute poolt kindlaks tehtud suurema riskiga juhtudel nõuavad liikmesriigid, et kohustatud isikud rakendavad klientide suhtes tugevdatud hoolsusmeetmeid, et asjakohaselt juhtida ja maandada kõnealuseid riske. Viies rahapesu direktiiv lisab artikli 18a, mistõttu muudeti ka neljanda rahapesu direktiivi artiklit 18, selliselt, et tugevdatud hoolsusmeetmeid kohaldatakse artiklites 18a – 24 sätestatud juhtudel. Artikkel 18a sätestab kohustatud isiku tegevused, kui tuleb kohaldada tugevdatud hoolsusmeetmeid. Kohustatud isikud peavad kohaldama tugevdatud hoolsusmeetmeid, kui ärisuhte või tehingu teine pool on komisjoni poolt määratud suure riskiga kolmandast riigist ning kohaldatavad meetmed on:

a. kliendi ja tegelikult kasu saava omaniku või omanike kohta lisateabe hankimine;
b. ärisuhte kavandatud olemuse kohta lisateabe hankimine;
c. kliendi ja tegelikult kasu saava omaniku või omanike vahendite allika ja vara allika kohta teabe hankimine;
d. kavandatud või sooritatud tehingute põhjuste kohta teabe hankimine;
e. ärisuhte loomiseks või jätkamiseks kõrgema juhtkonna[46] heakskiidu hankimine;
f. ärisuhte tugevdatud seire, suurendades kohalduvate kontrollide arvu ja ajastust ning valides välja täiendavat uurimist vajavad tehingumustrid.

[44] *Ibid.* Lk 58.
[45] Komisjoni delegeeritud määrus (EL) 2016/1675, 14.07.2016, millega täiendatakse Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/849, määrates kindlaks suure riskiga kolmandad riigis, kus esineb strateegilisi puudusi. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32016R1675&from=ET (14.04.2021).
[46] Neljanda rahapesu direktiivi põhjenduspunkti nr 34 kohaselt ei tähenda ''kõrgem juhtkond'' tingimata kooskõlastamist juhatusega. Pigem tähendab see seda, et kooskõlastuse peab andma selline isik, kellel on piisavad teadmised rahapesu ja terrorismi rahastamise riskidest ning on piisavalt kõrgel ametikohal selliste riske mõjutavate otsuste tegemiseks.

Sama artikli teine lõige sätestab, et lisaks eelnimetatud meetmetele, peavad kohustatud isikud komisjoni poolt suure riskiga riikidest pärit kliente hõlmavaid tehinguid füüsiliste või juriidiliste isikute suhtes, kasutusele võtma vähemalt ühe täiendavatest riskide maandamise meetmetest:

a. tugevdatud hoolsusmeetmete lisaelementide kohaldamine;
b. tugevdatud asjakohaste aruandlusmehhanismide või süstemaatilise finantstehingute aruandluse kasutusele võtmine;
c. ärisuhte või tehingute piiramine komisjoni poolt tuvastatud suure riskiga kolmandate riikidest pärit füüsiliste või juriidiliste isikutega.

Finantsinspektsiooni juhise kohaselt on tugevdatud hoolsusmeetmeks alati hiljemalt kuus kuud pärast ärisuhte loomist kliendi riskiprofiili uuesti hindamine. Tegeliku kasusaajate tuvastamise osas täpsustab Finantsinspektsioon, et ärisuhte loomisel võiks tuvastada ka selliste kasusaajate isikusamasus, kelle osalus on alla 25%.[47]

Tugevdatud hoolsusmeetmete kohaldamisele eelneb, nagu lihtsustatud hoolsusmeetmete kohaldamiselegi, riskihinnang. Neljanda rahapesu direktiivi art 18 lg 3 viitab direktiivi lisale III, milles on loetletud võimalikud suuremat riski iseloomustavad asjaolud:

1) klientidega seotud riskitegurid:
   a. ärisuhe toimib ebatavalistel asjaoludel;
   b. kliendid, kes on geograafilise riskiteguri tõttu kõrgema riskiga geograafiliste piirkondade residendid;
   c. juriidilised isikud või õiguslikud üksused, mis on personaalse varahalduse üksused;
   d. äriühingud, kellel on variaktsionärid või esitajaaktsiad;
   e. suuri sularahakoguseid käsitlevad ettevõtjad;
   f. äriühingu omandistruktuur näib äriühingu tegevust silmas pidades ebatavaline või liiga keeruline.
2) toote, teenuse, tehingu või edastamiskanaliga seotud riskitegurid:
   a. privaatpangandus;
   b. tooted või tehingud, mis võivad soodustada anonüümsust;
   c. ärisuhe või tehingud, mille puhul ei viibita samas kohas ja ei võeta teatavaid kaitseabinõusid, nagu elektrooniline allkirjastamine;

[47] Finantsinspektsiooni juhend (viide nr nr 4). Lk 58.

d. tundmatutelt või mitte seotud kolmandatelt isikutelt saadud maksed;
e. uues tooted ja äritavad, sealhulgas uus edastamismehhanism, ning uue või areneva tehnoloogia kasutamine nii uute kui ka olemasolevate toodete puhul.

3) geograafilised riskitegurid;

a. riigid, kus usaldusväärsete allikate kohaselt ei ole kehtestatud rahapesu ja terrorismi rahastamise tõkestamise tõhusaid süsteeme;
b. riigid, kus usaldusväärse allikate kohaselt on korruptsiooni või muu kuritegeliku tegevuse tase märkimisväärne;
c. riigid, kelle suhtes on kehtestatud sanktsioonid, embargo või sarnased meetmed, näiteks Euroopa Liidu või Ühinenud Rahvaste Organisatsiooni (ÜRO) poolt;
d. riigid, kes rahastavad või toetavad terrorismi või kelle territooriumil tegutsevad kindlaks määratud terroristlikud organisatsioonid.

Nagu eelnevalt mainitud, tähendab tugevdatud hoolsusmeetmete kohaldamine seda, et lisaks üldistele hoolsusmeetmetele, tehakse miskit lisaks. Krediidiasutused ja muud kohustatud isikud peavad, nii palju kui mõistlikult võimalik, uurima ning analüüsima klientide keerulisi omandistruktuure (juriidiliste isikute puhul), klientide ebatavaliselt suuri tehinguid ja kõiki ebatavalisi tehingute mustreid, millel ei ole selget majanduslikku või õiguspärast eesmärki[48]. Täpsemalt peaksid kohustatud isikud tihedamini monitoorima selliste klientide ärisuhet, et aru saada, kas sellised tehingud või muud toimingud on kahtlased[49].

Krediidiasutustel tuleb tugevdatud hoolsusmeetmeid kohaldada korrespondentsuhte[50] puhul. Lisaks üldistele hoolsusmeetmetele, tuleb krediidiasutustel teha järgmist:

a. koguvad piisavalt teavet respondentasutuse kohta, et täielikult mõista respondentasutuse tegevuse olemust ja teha avalikult kättesaadava teabe põhjal otsus asjaomase asutuse maine ja järelevalve kvaliteedi üle;
b. hindavad korrespondentasutuses rakendatavaid rahapesu ja terrorismi rahastamise tõkestamise kontrollsüsteeme;
c. saavad kõrgemalt juhtkonnalt eelnevalt nõusoleku uue korrespondentsuhte loomiseks;

[48] Fratangelo., P. Lk 18.
[49] *Ibid.* Lk 18.
[50] Neljanda rahapesu direktiivi art 3 p 8 kohaselt on korrespondentsuhe pangateenuse osutamine ühe panga (''korrespondentpank'') poolt teisele pangale (''respondentpank''), sh arvelduskonto või muu passivakonto ning seonduvate teenuste osutamine, nagu rahahaldus, rahvusvahelised rahaülekanded, tšekkide lunastamine, laiendatud kasutusõigusega kontod ja valuutavahetusteenused. Samuti on korrespondentsuhet defineeritud kui suhteid krediidiasutuste ja finantseerimisasutuste vahel, sealhulgas sellised suhted, mille puhul korrespondentpank osutab respondentpangale sarnaseid teenuseid, ning sellised suhted, mis on loodud väärtpaberitehingute või rahaülekannete tegemiseks.

d. dokumenteerivad mõlema asutuse vastavad kohustused;
e. veenduvad laiendatud kasutusõigusega kontode puhul, et respondentasutus on kontrollinud korrespondentasutuse kontodele otsest juurdepääsu omavate klientide isikusamasus ning võtab nende suhtes pidevalt hoolsusmeetmeid ning suudab taotluse korral esitada asjakohaseid kliendi suhtes rakendatavate hoolsusmeetmete andmed.

Krediidiasutused ehk korrespondendid peavad rakendama eelnimetatud tugevdatud hoolsusmeetmeid neis riikides asuvate respondentasutuste suhtes, kes asuval väljaspool Euroopa Majanduspiirkonda (EMP). Siiski võivad korrespondendid, tulenevalt riskiisust, kohandada tugevdatud hoolsusmeetmete ulatust. Kui krediidiasutus on asjakohaste uuringute tulemusel veendunud, et respondentasutus asub kolmandas riigis, kus on tõhus rahapesu ja terrorismi tõkestamise kord, mille vastavust Euroopa Liidus kehtivatele nõuetele pidevalt kontrollitakse ja puudub põhjus kahelda, et respondentasutuse rahapesuvastased poliitika ja protseduurid on ebapiisavad või on hiljuti ebapiisavaks tunnistatud, siis on võimalik, et respondentasutuse rahapesuvastaseid kontrollimeetmeid ei pea hindama üksikasjalikult. Kui respondentasutus asub EMP riigis, ei tähenda see automaatselt, et hoolsusmeetmeid kohaldada ei ole vaja. Selliste respondentasutuste suhtes tuleb siiski kohaldada üldiseid hoolsusmeetmeid. Kui EMP riigis asuva respondentasutusega seotud risk on suurenenud, tuleb tema suhtes rakendada tugevdatud hoolsusmeetmeid. Eelkõige tuleks koguda täiendavat ning piisavat teavet respondentasutuse kohta, et selle asutuse tegevuse olemust täielikult mõista (art 19 p a) ning hinnata korrespondentsasutuses rakendatavaid rahapesu ja terrorismi rahastamise tõkestamise kontrollsüsteeme.[51]

Neljanda rahapesu direktiivi artikkel 24 sätestab, et krediidiasutustel ega finantseerimisasutustel ei ole lubatud luua ega jätkata korrespondentsuhteid varipankadega. Samuti ei või krediidiasutused ega finantseerimisasutused luua ega jätkata korrespondentsuhteid asutustega mis teadaolevalt lubavad varipankadel oma kontosid kasutada. Varipank on neljanda rahapesu direktiivi artikli 3 p 17 kohaselt krediidi- või finantseerimisasutus või krediidiasutuste ja investeerimisasutustega samaväärseid toiminguid tegev asutus, mis on asutatud jurisdiktsioonis, kus tal puudub füüsiline asukoht sihipärase kontseptsiooni ja juhtimisega, ja mis ei ole seotud ühegi reguleeritud finantskontserniga. Seega

[51] Euroopa Pangandusjärelevalve. Direktiivi (EL) 2015/849 artikli 17 ja artikli 18 lõike 4 alusel koostatud ühissuunised, milles käsitletakse kliendi suhtes rakendatavaid lihtsustatud ja tugevdatud hoolsusmeetmeid ning tegureid, mida krediidi- ja finantseerimisasutused peaksid arvesse võtma, kui nad hindavad üksikute ärisuhete ja juhutehingutega seotud rahapesu ja terrorismi rahastamise riski. Suunised riskitegurite kohta. 04.01.2018, lk 31 – 32. Arvutivõrgus: https://www.fi.ee/sites/default/files/2018-08/pp_nr_10_Guidelines_on_Risk_Factors_ET_04-01-2018.pdf (14.03.2021)

on varipank lihtsalt üks abstraktne juriidiline isik, mis ei allu ühelegi regulatsioonile või allub vaid üksikutele regulatsioonidele. Varipanganduse oht seisneb selles, et nende kohta ei ole võimalik saada vajalikku ja usaldusväärset informatsiooni asutuse tegutsemise või varade kohta ja selle tõttu on riskid liiga suured[52]. Samuti ei ole varipankade üle võimalik teostada efektiivset järelevalvet.

Lisaks varipankadele tehakse tehinguid ka *shell bank* ehk riiulipankade kaudu. *Shell bank* on nii-öelda pank, mis füüsiliselt ei paikne üheski jurisdiktsioonis ja seetõttu on selliste äriühingute probleemiks kontrolli ja vastutuse hägune ja arusaamatu jagunemine[53]. Tõenäoliselt on just eelnimetatud probleemide tõttu Euroopa Liidu tasandil keelatud selliste äriühingutega ärisuhete loomine. Vastupidine tegevus läheks täielikult vastuollu Euroopa Liidu ja FATF'i suuniste ja põhimõtetega, mille kohaselt ei ole võimalik tagada finantssektori läbipaistvust tehes tehinguid äriühingutega, mille olemusest pole võimalik aru saada.

Lisaks on neljanda rahapesu direktiivi artiklites 20 – 23 reguleeritud krediidiasutuste tegevus, kui ärisuhe luuakse või tehakse tehing riikliku taustaga isikuga. Riikliku taustaga isik (PEP[54]) direktiivi artikli 3 punkti 9 järgi füüsiline isik, kes täidab või on täitnud avaliku võimu olulisi ülesandeid. Sellisteks isikuteks on sealhulgas: riigipea, valitsusjuht, minister ning ase- või abiministrid, parlamendiliikmed, erakondade juhtorganite liikmed, ülemkohtute, konstitutsioonikohtute liikmed, kelle otsuseid saab edasi kaevata vaid erandjuhtudel, riigikontrolliasutuste ja keskpankade nõukogude liikmed, suursaadikud ja kaitsejõudude kõrgemad ohvitserid, riigiettevõtete juhatuse või järelevalveorganite liikmed või rahvusvahelise organisatsiooni juhid, juhi asetäitjad ja juhtorgani liikmed. RahaPTS § 9^1 lg 5 alusel on rahandusministeerium koostanud nimekirja ametikohtadest[55], mille täitjaid loetakse Eestis riikliku taustaga isikuteks.

Selliste isikute suhtes tuleb krediidiasutustel lisaks üldistele hoolsusmeetmete rakendamisele:

a. luua asjakohane riskijuhtimissüsteem, sh riskipõhised protseduurid, millega tehakse kindlaks, kas klient või kliendi tegelikult kasu saav omanik on riikliku PEP;

[52] Seletuskiri rahapesu ja terrorismi rahastamise tõkestamise seaduse eelnõu juurde. Lk 38 – 39. Arvutivõrgus: https://m.riigikogu.ee/tegevus/eelnoud/eelnou/fb03e20e-caf7-463d-9b60-ddf6021742b2/Rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20seadus (14.03.2021).
[53] *Ibid.*
[54] Ingl. *politically exposed person* .
[55] Rahandusministri 27.09.2020 määrus. Loetelu Eesti ametikohtadest, mille täitjaid loetakse riikliku taustaga isikuteks. RT I, 24.09.2020, 4.

b. võtta ärisuhetes PEP-iga kasutusele järgmisi meetmeid:
    i) saavad kõrgemalt juhtkonnalt heakskiidu sellise isikuga ärisuhte loomiseks või jätkamiseks;
    ii) võtavad asjakohaseid meetmeid, et teha kindlaks sellise vara ja selliste rahaliste vahendite allikad, mida selliste isikutega ärisuhetes või tehingute tegemisel kasutatakse;
    iii) teostavad selliste ärisuhete pidevat tugevdatud seiret.

Riikliku taustaga isiku puhul on krediidiasutustel kohustus võtta kasutusele mõistlikke meetmeid, et teada saada, kas kindlustuslepingute puhul (elukindlustus või investeerimisriskiga kindlustus) on soodustatud isikuks või soodustatud isiku tegelikult kasu saav omanik riikliku taustaga isik. See teave tuleb krediidiasutusel välja selgitada hiljemalt siis, kui tehakse kindlustuslepingu järgne väljamakse. Kui krediidiasutused näevad suurema riski olemasolu, tuleb lisaks üldistele hoolsusmeetmetele teavitada krediidiasutuse kõrgemat juhtkonda enne väljamakse tegemist ning tuleb üksikasjalikult kontrollida kogu ärisuhet kindlustusvõtjaga (art 21).

Neljanda rahapesu direktiivi artikkel 23 sätestab, et lisaks kohaldatakse tugevdatud hoolsusmeetmeid ka riikliku taustaga isikute pereliikmete või isikute suhtes, kes on riikliku taustaga isiku lähedased kaastöötajad. Direktiivi artikkel 3 p 10 järgi on PEP-i lähedaseks isikuks abikaasa või abikaasaga samaväärseks peetav isik, lapsed ja nende abikaasad või abikaasaga samaväärne isik ja PEP-i vanemad. PEP-i lähedaseks kaastöötajaks on direktiivi artikli 3 p 10 kohaselt füüsiline isik, kellest on teada, et ta on juriidilise isiku või õigusliku üksuse tegelikult kasu saav ühine omanik koos riikliku taustaga isikuga või kellel on lähedased ärisuhted riikliku taustaga isikuga. Samuti on lähedane kaastöötaja füüsiline isik, kes on sellise juriidilise isiku või õigusliku üksuse ainus kasu saav omanik, mis on teadaolevalt tegelikult asutatud riikliku taustaga isiku kasuks.

Riikliku taustaga isiku puhul on ühiskonnas tegemist isikutega, kellele antakse võimalus teha otsuseid riigi tasandil ja seetõttu peaks sellistel isikutel olema suurem rahvapoolne usaldus, eriti neil ametikohtadel, kuhu valib ametniku rahvas. Kui selline isik on kuidagi seotud tegevusega või äriühingutega, millel on seos rahapesu või terrorismi rahastamisega, võib ärisuhe sellise isikuga krediidiasutusele kaasa tuua tõenäoliselt juriidilisi probleeme, kuid ka mainekahju. Mainekahju võib autori arvates krediidiasutusele olla isegi suuremaks ohuks, kuna

krediidiasutuste ning nende klientide vaheline suhe baseerub autori arvates suurel määral usaldusel.

Nagu autor on eelnevalt selgitanud, tähendab tugevdatud hoolsusmeetmete kohaldamine seda, et andmeid isiku kohta kogutakse rohkem ning tihemini, kui üldiste hoolsusmeetmete kohaldamisel, mis võib üldsusele anda indikatsiooni, et selliste isikutega kaasnevad suuremad riskid rahapesu või terrorismi rahastamise osas. Tugevdatud hoolsusmeetmete kohaldamine on siiski vaid ennetav meede ning ei tohi olla riikliku taustaga isiku suhtes kriminaliseeriv ning tugevdatud hoolsusmeetmete kohaldamist ei tohiks tõlgendada nii, et riikliku taustaga isikule jääks külge märk kui kriminaalses tegevuses osaleva isikule[56]. Autori arvates kohaldub eeltoodu ka riikliku taustaga isiku pereliikmete kui ka lähedaste kaastöötajate suhtes. Ka neile ei tohiks jääda külge märki, et nad oleksid kuidagi seotud rahapesu või terrorismi rahastamisega vaid seetõttu, et nad on riikliku taustaga isiku pereliikmed või kolleegid.

Tugevdatud hoolsusmeetmete kohaldamine riikliku taustaga isikute, nende pereliikmete või lähedaste kaastöötajate osas ei toimu igavesti ega ka nii kaua, kuniks riikliku taustaga isik, tema pereliige või lähedane kaastöötaja on kohustatud isiku klient. Neljanda rahapesu direktiivi artikkel 22 sätestab, et kui isik ei ole enam riikliku taustaga isik, tuleb kohustatud isikutel vähemalt 12 kuu jooksul võtta arvesse riske, mis on riikliku taustaga isikuga endiselt seotud ja rakendada asjakohaseid ja riskitundlikkusest tulenevaid meetmeid seni, kuni on kindel, et riikliku taustaga isikutele omaseid riske selle isiku puhul enam ei esine. Autori arvates ei tähenda eeltoodu seda, et riikliku taustaga isiku osas peaks minimaalselt aasta vältel pärast tema ametiaja lõppemist kohaldama samu tugevdatud hoolsusmeetmeid, mida kohaldati selle aja vältel, kui riikliku taustaga isik oli ametis. Selleks ongi direktiiviga antud kohustatud isikutele võimalus oma riskiisust tulenevalt otsustada, milliseid hoolsusmeetmeid, lisaks üldistele hoolsusmeetmetele, selliste isikute suhtes edaspidiselt kohaldada. Hoolsusmeetmed, mida kohustatud isik, sh krediidiasutus edaspidi kohaldab, oleneb suuresti kohustatud isiku riskiisust. Kohaldatavad hoolsusmeetmed erinevad ka isikupõhiselt, kuna iga riikliku taustaga isiku puhul tuleb hinnata riske eraldi, seega tuleb ka pärast riikliku taustaga isiku ametiaja lõppemist otsustada, milliseid hoolsusmeetmeid kohaldada, konkreetsest isikust tulenevaid riske hinnates. Direktiivi kohaselt tuleb hoolsusmeetmeid kohaldada vähemalt 12 kuud pärast ametiaja lõppemist, kuid direktiiv ei sätesta maksimaalset ajaperioodi, millal asjakohaste hoolsusmeetmete kohaldamine lõpetamine toimuma peaks. Selle asemel sätestab direktiiv, et

[56] (EL) 2018/849. Põhjenduspunkt nr 33.

selliseid meetmeid tuleb kohaldada senikaua kuni endisest riikliku taustaga isikust ei tulene enam rahapesu ja terrorismi rahastamise alaseid riske. Sellest võib järeldada, et krediidiasutustel, kohustatud isikuna, on võimalus kohaldada tugevdatud hoolsusmeetmeid ka aastaid pärast riikliku taustaga isiku ametiaja lõppemist.

Eelkirjutatust nähtub, et rahapesu ja terrorismi rahastamise tõkestamisel on kohustatud isikutel, sh krediidiasutustel täita oluline roll. Selleks, et tagada finantssektori läbipaistvus, tuleb kohustatud isikutel täita hoolsusmeetmeid nii ärisuhte alguses kui ka selle kestel. Ärisuhte alguses hoolsusmeetmete kohaldamine on oluline, et takistada juba eos kriminaalse päritoluga raha ringlusesse sattumist. Ärisuhte kestel hoolsusmeetmete kohaldamise eesmärgiks on, et kui juhuslikult on sattunud kriminaalse päritoluga raha ringlusesse, siis seda märgataks esimesel võimalusel, samuti märgatakse ärisuhte seire kestel kahtlaseid tehinguid ärisuhte ajal, mis samuti takistab kriminaalse päritoluga raha ringlemist.

Siiski tuleb rahapesu ja terrorismi rahastamise tõkestamiseks koguda palju teavet, sh töödelda, koguda ja säilitada isikuandmeid. Kuna hoolsusmeetmete mittekohasel täitmisel on kohustatud isikute jaoks üsna rasked tagajärjed suurte rahatrahvide näol[57] või ähvardava mainekahju näol, võivad krediidiasutused igaks juhuks koguda ja töödelda rohkem isikuandmeid, kui seda lubab seadus. Siiski ei tohi ära unustada seda, et lisaks rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmete kohaldamiseks kohustatud isikule on need isikud ka vastutavad isikuandmete töötlejad ning liigsel hulgal isikuandmeid kogudes ja neid töödeldes, riskivad kohustatud isikud sellega, et nad riivavad liigselt oma klientide ehk andmesubjektide õigusi isikuandmete kaitsele. Ka isikuandmete kaitse normide rikkumisel on üsna rasked tagajärjed. Nimelt on ka selles valdkonnas kehtestatud suured rahalised karistused.

Järgmistes peatükkides kirjeldab autor milliste piirangutega peavad krediidiasutused arvestama, kui nad töötlevad isikuandmeid rahapesu hoolsusmeetmete täitmisel.

[57] Neljanda rahapesu direktiivi artikli 59 lg 2 p e) kohaselt on maksimaalne rahaline karistus hoolsusmeetmete kohaldamise rikkumisel vähemalt kahekordne kasu, mis saadi õigusrikkumise tulemusel või vähemalt 1 000 000 eurot. RahaPTS § 82 lg 2 järgi on hoolsusmeetmete kohaldamise rikkumise eest juriidilisele isikule kohaldatav rahatrahv kuni 400 000 eurot.

2. ÕIGUS ISIKUANDMETE KAITSELE

Käesolevas peatükis kirjeldab autor isikuandmete mõistet, isikuandmete määratletust õigusaktides. Samuti kirjeldab autor isikuandmete kaitse olulisi põhimõtteid, täpsemalt: eesmärgipärasus, minimaalsus ning õigsus. Autori arvates haakuvad just need kolm printsiipi isikuandmete töötlemisega rahapesu hoolsusmeetmete rakendamisel. Lisaks analüüsib autor, kas ja millisel määral põrkuvad need printsiibid rahapesu ja terrorismi rahastamise hoolsusmeetmete rakendamisel peamise printsiibiga, milleks on võimalikult palju teabe ning andmete kogumine. Kuna isikuandmete kaitse on rahapesu ja terrorismi rahastamise kõrval teine päevakajaline teema Euroopa Liidus, on autori arvates oluline esmalt selgitada millised on isikuandmete kaitse õiguse peamised printsiibid ning miks õigust isikuandmete kaitsele niivõrd oluliseks pidada tuleb.

2.1. Isikuandmete mõiste ja määratletus õigusaktides

Isikuandmete definitsioon on isikuandmete kaitse üldmääruse (edaspidi GDPR[58]) art 4 kohaselt igasugune teave tuvastatud või tuvastatava isiku (''andmesubjekti'') kohta. Tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või sellise füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal (art 4 p 1). Kuna käesolev magistritöö käsitleb osaliselt ka andmete kogumist juriidiliste isikute osas, peab autor vajalikuks märkida, et kuivõrd juriidilisel isikul eraelu puudub (mille kaitse alla kuulub mh õigus isikuandmete kaitsele), ei ole juriidilisel isikul isikuandmeid ning GDPR kohaldub vaid füüsilistele isikutele. Juriidiliste isikute puhul kohaldub GDPR vaid siis, kui juriidilise isiku nimes on üks või mitu füüsilise isiku nime[59]. Eestis peab füüsilisest isikust ettevõtjal äriseadustiku[60] § 8 lg 1 alusel tema ärinimi sisaldama ettevõtja ees- ja perekonnanime, välja arvatud siis, kui füüsilisest isikust ettevõtja on talupidaja ja ärinimes sisaldub talu nimi (§ 8 lg 2). Seega kohaldub GDPR Eestis igale füüsilisest isikust ettevõtjale, ülejäänud äriühingute vormide osas saab omanik ise ärinime otsustada ja sellega seoses omakorda otsustada, kas lisada isikuandmed ärinimele või mitte.

[58] General Data Protection Regulation (viide nr 7).
[59] EKo liidetud kohtuasjad C-92/09 ja C-93/09 *Volker und Markus Schenke GbR ja Hartmut Eifert vs Land Hessen*, ECLI:EU:C:2010:662. p 53.
[60] RT I, 04.01.2021, 46

Eestis reguleerib isikuandmete kaitset isikuandmete kaitse seadus (edaspidi IKS[61]).

Eelnevast tulenevalt saab öelda, et isikuandmete mõiste on omajagu lai, GDPR'i mõttes võib isikuandmetena käsitleda nii isikukoodi, sõrmejälge, videot, pilti või isegi helisalvestist, ehk põhimõtteliselt kõiki andmeid, mille abil saab füüsilist isikut tuvastada. Käesolevas magistritöös keskendub autor selliste isikuandmete kogumisele ning töötlemisele, mida kasutatakse rahapesu ja terrorismi rahastamise tõkestamiseks. Sellisteks isikuandmeteks on eelkõige nimi, isikukood, või asukohateave.

Isikuandmete kaitse põhiõigust kui sellist ei käsitle Eesti Vabariigi põhiseadus (edaspidi PS[62]). Siiski saab isikuandmete kaitse paigutada PS § 26 kaitsealasse. PS § 26 sätestab, et igaühel on õigus perekonna- ja eraelu puutumatusele. Riigiasutused, kohalikud omavalitsused ja nende ametiisikud ei tohi kellegi eraellu sekkuda muidu, kui seaduses sätestatud juhtudel. Riigikohus on asunud seisukohale, et isikuandmete varjatud töötlemine riivab PS § 26 lg-s 1 sätestatud perekonna- ja eraelu puutumatust, mis üldsättena kaitseb kogu eraelu ning varjatud andmete töötlemine võib tähendada intensiivset sekkumist isiku õigustesse[63]. Ei ole põhjust asuda seisukohale, et isikuandmete töötlemine, mis ei ole varjatud, ei riivaks PS § 26 lg-s 1 sätestatud õigusi üldse. Varjatud andmete töötlemine toimub isiku teadmata, mis riivab tema õigusi rohkem, kui andmete töötlemine, millest isik on teadlik. Seega on Riigikohus tunnustanud, et isiku õigus tema isikuandmete kaitsele kuulub PS § 26 kaitsealasse.

PS § 26 sõnastusel on eeskuju võetud Euroopa Inimõiguste ja Põhivabaduste Kaitse Konventsiooni (edaspidi EIÕK[64]) artiklist 8, mille kohaselt on igaühel õigus sellele, et austataks tema era- ja perekonnaelu ja kodu ning sõnumite saladust[65]. Euroopa Inimõiguste kohus (edaspidi EIK) on selgitanud, et eraelu on niivõrd lai mõiste ning seda pole võimalik konkreetselt määratleda[66]. Autori arvates sobitub õigus isikuandmete kaitsele kõige paremini eraelu kaitsealasse. Samale seisukohale on asunud Euroopa Inimõiguste kohus (edaspidi EIK). EIK on selgitanud, et isikuandmete kaitse on fundamentaalse tähtsusega isiku eraelu kaitsel, millele viitab ka EIÕK artikkel 8[67].

[61] RT I, 04.01.2019, 11.
[62] RT I, 15.05.2015, 2.
[63] RKPJKo 5-19-38. p 95, 98.
[64] RT II 2010, 14, 54.
[65] Madise, Ü. PSK § 26/2. – Eesti Vabariigi põhiseadus. Komm vlj. 5. vlj. Tallinn: Juura 2020. Arvutivõrgus: https://pohiseadus.ee/sisu/3497/paragrahv_26 (15.03.2021).
[66] EIKo 44599/98, *Bensaid v. the United Kingdom.* p 47.
[67] EIKo 30562/04, *S. and Marper v. the United Kingdom.* p 103.

PS § 26 kaitsealasse kuulub ka isiku informatsiooniline enesemääramine. See tähendab, et igaühel on õigus ise otsustada, kas tema kohta kogutakse ja töödeldakse andmeid ja kui palju seda tehakse, mistõttu on eraelu kaitse oluline valdkond just isikuandmete kaitse[68]. Isikuandmete kaitset on käsitlenud ka Riigikohtu halduskolleegium, selgitades, et ''eraelu puutumatuse riivena käsitatakse muu hulgas isikuandmete kogumist, säilitamist, kasutamist ja avalikustamist''[69].

Eraelu puutumatus, mis on PS §-s 26 sätestatud ei ole siiski absoluutne õigus. Sätte teine lause sätestab piiriklausli, mille kohaselt võib eraellu sekkuda seaduses sätestatud juhul või kui see on vajalik tervise, kõlbluse, avaliku korra või teiste inimeste õiguste või vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks. Seega saab isiku eraellu sekkuda vaid siis, kui selleks annab loa seadus või põhiseaduses endas kirjeldatud juhtudel. Kuna õigus isikuandmete kaitsele kuulub § 26 kaitselasse, saab ka õigust isikuandmete kaitsele piirata vaid eelnimetatud juhtudel.

Isikuandmete kaitset kui põhiõigust käsitleb kõige konkreetsemalt Euroopa Põhiõiguste Harta (edaspidi harta)[70]. Harta art 8 lg 1 kohaselt on igaühel õigus oma isikuandmete kaitsele. Sätte teine lõige sätestab isikuandmete töötlemise alused ja üldpõhimõtted. Nimelt võib isikuandmeid töödelda asjakohaselt ning kindlaksmääratud ja asjaomase isiku nõusolekul või muul seaduses sätestatud õiguslikul alusel. Sellest nähtub, et kui isikuandmete töötlemiseks puudub andmesubjekti nõusolek, tuleb isikuandmete töötlemiseks leida seadusest tulenev alus. Sarnaselt hartale nimetab õiguse isikuandmete kaitsele ka Euroopa Liidu Toimimise Lepingu (edaspidi ELTL) art 16[71].

Seega on õigus isikuandmete kaitsele tunnustatud ning olulise kaaluga põhiõigus ja seda võib riivata vaid siis, kui selleks annab loa õigusakt. Erandina on Riigikohus tunnistanud, et eraellu saab sekkuda ka põhiseaduse preambulis sätestatud väärtuste kaitseks[72].

Järgnevalt kirjeldab autor isikuandmete töötlemise põhimõtteid ning analüüsib, millistes olukordades võib tekkida oht riivata isiku õigusi isikuandmete kaitsele eriti intensiivselt, kui

[68] Madise, PSK § 26/24.
[69] RKHKo 3-3-1-3-12, p 19.
[70] Euroopa Liidu Põhiõiguste harta. – ELT C/83. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:12010P&from=EN.
[71] Euroopa Liidu Toimimise Lepingu Konsolideeritud Versioon. – ELT C/326. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:12012E/TXT&from=ET.
[72] RKPJKo 3-4-1-6-01. p 18.

krediidiasutused töötlevad isikuandmeid ka rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmeid täites.

2.2. Isikuandmete töötlemise põhimõtted: eesmärgipärasus, minimaalsus ning õigsus

Isikuandmete töötlemine on GDPR- i artikli 4 p 2 järgi isikuandmete või nende kogumiga tehtav automatiseeritud või automatiseerimata toiming või toimingute kogum, nagu isikuandmete kogumine, dokumenteerimine, korrastamine struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamise, edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine. Sellest nähtub, et isikuandmete töötlemine on põhimõtteliselt iga tegevus, mis sisaldab isikuandmeid.

Käesolevas alapeatükis käsitleb autor kolme isikuandmete töötlemise põhimõtet, mis on autori arvates kõige rohkem seotud käesoleva magistritööga. GDPR art 5 lg 1 nimetab kuus isikuandmete töötlemise põhimõtet: isikuandmete töötlemise seaduslikkus, õiglus ning läbipaistvus, eesmärgipärasus, võimalikult väheste andmete kogumine, isikuandmete õigsus, isikuandmete säilitamise piirang ning usaldusväärsus ja konfidentsiaalsus. Käesolevas alapeatükis käsitleb autor eelnimetatutest kolme isikuandmete töötlemise põhimõtet: eesmärgipärasus, andmete töötlemise minimaalsuse printsiip ning andmete õigsuse printsiip. Autori arvates on need kolm põhimõtet kõige rohkem seotud krediidiasutuste poolt kohaldatavate rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmetega. Autor peab vajalikuks märkida, et kõik GDPR-is sätestatud isikuandmete töötlemise printsiibid on omavahel osaliselt põimunud ning erinevate printsiipide sisu võib omavahel kattuda. Näiteks tuleks autori hinnangul koos rakendada läbipaistvuse põhimõtet ning eesmärgipärasuse põhimõtet: isikuandmete töötlemise eesmärgid peavad olema konkreetsed ja arusaadavad ja lisaks ka läbipaistvad. Ehk andmesubjekt peab aru saama millisel eesmärgil tema isikuandmeid töödeldakse ja see eesmärk peab olema läbipaistev, et vastutavad töötlejad ei saaks isikuandmeid töödelda eesmärkidel, mis on muuhulgas hägused ja arusaamatud.

2.2.1. Isikuandmete töötlemise eesmärgipärasus

GDPR. Art 5 lg 1 p b) näeb ette, et isikuandmeid kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning neid ei töödelda hiljem viisil, mis on nende eesmärkidega

vastuolus (''eesmärgi piirang''). Eesmärgipärasuse printsiibis on nähtavasti kaks komponenti: esiteks peab vastutav töötleja koguma ainult isikuandmeid konkreetse ja õiguspärase eesmärgiga, teiseks, kui isikuandmed on kogutud, ei tohi neid edaspidi töödelda sellisel viisil, mis on vastuolus eesmärgiga, milleks isikuandmeid esmalt koguti[73]. Seega kui vastutav töötleja töötleb esialgu kogutud isikuandmeid erineval eesmärgil, peab vastutaval töötlejal olema isikuandmete töötlemiseks olema omakorda seaduslik alus. Vastutav töötleja ei saa edaspidist andmete töötlemist õigustada sellega, et esialgne andmete kogumine ja töötlemine oli õiguspärane.

Isikuandmete töötlemisel tuleb seega kindlaks määrata konkreetsed eesmärgid, milleks neid kogutakse ja töödeldakse. Samuti tuleb need eesmärgid teatavaks teha andmesubjektile, kuna regulatsiooni eesmärk on kaitsta just andmesubjekti ning kuna andmesubjektil on õigus teada, milliseid andmeid tema kohta kogutakse, peab olema andmesubjektil autori arvates ka õigus teada mille jaoks neid andmeid kogutakse. Eesmärkide kirjeldamisel on oluline ka see, et seatud eesmärgid oleks piisavalt täpsed ning arusaadavad, et neist saaks lisaks vastutavale töötlejale ning tema töötajatele aru ka kolmandad isikud, kes isikuandmeid töötlevad, isikuandmete kaitsega seotud ametiasutused ning andmesubjekt ise samuti[74]. Eriti tähelepanelik tuleb olla selliste andesubjektide suhtes, kellel võib olla erinev keeleline või kultuuriline taust ja sellest tulenevalt ei pruugi andmesubjektid tavapärasest selgitusest piisavalt aru saada[75]. Euroopa Andmekaitseinspektor on oma arvamuses selgitanud, et kogutud isikuandmete töötlemine täiesti teistsugusel eesmärgil, mis ei ole esialgsega üldsegi seotud, on rikub isikuandmete eesmärgipärasuse põhimõtet ning ähvardab ka proportsionaalsuse põhimõtte implementeerimist[76].

Harta artikkel 52 lg 1 näeb ette, et hartas tunnustatud õiguste ja vabaduste teostamist tohib piirata ainult seadusega ning arvestades nimetatud õiguste ja vabaduste olemust. Proportsionaalsuse põhimõtte kohaselt võib piiranguid seada üksnes juhul, kui need on vajalikud ning vastavad tegelikult liidu poolt tunnustatud üldist huvi pakkuvatele eesmärkidele või kui on vaja kaitsta teiste isikute huvi ja vabadusi. Seega peab riive isikuandmete kaitse

[73] Article 29 Data Protection Working Party (edaspidi WP29). Opinion 03/2013 on purpose of limitation. Lk 4. Arvutivõrgus: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (15.03.2021).
[74] *Ibid.* Lk 17.
[75] *Ibid.*
[76] European Data Protection Supervisor. Opinion on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC, Access to beneficial ownership information and data protection implications. 02.02.2017. Lk 9. Arvutivõrgus: https://edps.europa.eu/sites/default/files/publication/17-02-02_opinion_aml_en.pdf (15.03.2021).

õigusele olema proportsionaalne. ELK on kohtuasjas *Digital Rights Ireland Ltd* selgitanud, et rahvusvaheline terrorismivastane võitlus rahvusvahelise rahu ja julgeoleku säilitamiseks on endast üldist huvi pakkuv liidu eesmärk[77]. Järelikult võib terrorismivastase võitluse hüvanguks riivata isikute põhiõigust isikuandmete kaitsele.

Eesmärgid, mille jaoks isikuandmeid edaspidi töötlema hakatakse, tuleb kindlaks määrata isikuandmete kogumise ajal[78]. Autori arvates tuleb kindlaks määratud eesmärke andmesubjektile tutvustada samal ajal, ehk andmete kogumise faasis, et andmesubjekt saaks hinnata, kas anda nõusolek (kui isikuandmeid kogutakse andmesubjekti nõusoleku alusel) isikuandmete edaspidiseks töötlemiseks või mitte.

Eesmärgid, mille jaoks isikuandmeid kogutakse ja töödeldakse peavad samuti olema õiguspärased. Õiguspärasuse kriteerium ning mõiste isikuandmete töötlemisel on laiem, kui isikuandmete kaitse direktiivi[79] artiklis 7 nimetatud isikuandmete töötlemise alused, millest vähemalt ühe täitmine muudab isikuandete töötlemise õiguspäraseks (samad isikuandmete töötlemise alused on kehtestatud GDPR-i artiklis 6. Õiguspärasus tähendab muuhulgas ka seda, et isikuandmete töötlemise eesmärgid peavad olema kooskõlas õigusaktidega. Õigusaktide all on mõeldud kõiki võimalikke õigusakte (seadused, määrused, kohalike omavalitsuste poolt kehtestatud õigusaktid, põhiseaduslikud printsiibid, põhiõigused ja muud õiguse printsiibid), mille kohaldamine on kohtutele õiguse mõistmisel siduv[80].

On arusaadav, et vastutavatel töötlejatel on oluliselt lihtsam kasutada juba kogutud isikuandmeid oma asutuse sees, kui neid andmesubjektilt uuesti küsida ning töödelda. See puudutab ka näiteks krediidiasutuste tegevust isikuandmete töötlemisel. Kui füüsiline isik ehk andmesubjekt soovib krediidiasutusest võtta laenu, tuleb selleks avaldada andmeid muuhulgas ka oma majandusliku seisukorra kohta. Sellised andmed võivad krediidiasutusele olla kasulikud ning vajalikud ka siis, kui sama füüsiline isik on näiteks sama krediidiasutuse teise kliendi tegelik kasusaaja ja sellise isiku suhtes tuleb kohaldada rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmeid. Sellisel juhul tõusetub küsimus sellest, kas krediidiasutus võib algselt kogutud isikuandmeid töödelda hoolsusmeetmete rakendamisel, või ei ole see enam kooskõlas esialgse andmete töötlemise eesmärgiga.

---

[77] EKo liidetud kohtuasjad C – 293/12 ja C – 594/12 *Digital Rights Ireland Ltd vs Minister for Communications jt,* ECLI:EU:C:2014:238. p 42 ja seal viidatud kohtupraktika.
[78] (EL) 2016/679. Põhjenduspunkt 39.
[79] Enne DGPR-i kohaldunud Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ. – ELT L 281. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:31995L0046&from=EN.
[80] WP29. Opinion 03/2013 (viide nr 73). Lk 19-20.

Selleks, et aru saada, kas edasise töötlemise eesmärk on esialgsest erinev, peaks vastutav töötleja pärast kõikide esialgsete isikuandmete töötlemise seaduslikkuse seisukohast vajalike nõuete täitmist, võtma arvesse ükskõik milliseid seoseid esialgse ja edaspidise isikuandmete töötlemise eesmärgi vahel ning isikuandmete kogumise konteksti[81]. Lisaks tuleks eelkõige arvesse võtta andmesubjekti mõistlikke ootusi andmete edasise kasutamise suhtes, isikuandmete laadi, kavandatava edasise töötlemise tagajärgi andmesubjekti jaoks ning asjakohaste kaitsemeetmete olemasolu nii esialgses kui ka edaspidises kavandatavas isikuandmete töötlemise toimingutes[82].

Autori arvates on siinkohal olulisim arvesse võtta andmesubjekti mõistlikke ootusi tema isikuandmete töötlemisel. Selleks tuleks iga kord küsida, et kas mõistlik isik saaks aru, et tema kohta esialgselt kogutud isikuandmeid töödeldakse teistsuguse eesmärgi nimel. Kui vastus on eitav, ei ole edaspidine isikuandmete töötlemine seaduslik, kuna isikuandmete töötlemine oleks esialgsest eesmärgist liialt erinev. Autori arvates ei suudaks keskmine laenutaotleja ette näha, et tema laenutaotluses edastatud isikuandmeid hakataks edaspidi töötlema ka rahapesu või terrorismi rahastamise tõkestamise eesmärgil. Eriti juhul, kui see sama füüsiline isik on sama krediidiasutuse teise kliendi tegelikult kasu saav omanik. Kui krediidiasutus rakendab rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmeid, tuleks sellise isiku andmeid koguda ja töödelda konkreetselt selle eesmärgiga. Selliseks uueks andmete kogumiseks ja töötlemiseks peab krediidiasutus leidma jällegi seadusliku aluse.

2.2.2. Isikuandmete töötlemise minimaalsuse printsiip

GDPR-i artikkel 5 lg 1 p c) järgi tagatakse isikuandmete töötlemisel, et isikuandmed on asjakohased, olulised ja piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt (''võimalikult väheste andmete kogumine''). Isikuandmete töötlemise minimaalsuse printsiip tähendabki, et isikuandmeid tuleb koguda nii palju kui vaja, kuid nii vähe kui võimalik. Eelkõige eeldab see seda, et tagatakse, et isikuandmete säilitamise aeg oleks rangelt minimaalne[83]. ELK on selgitanud, et direktiivi artikli 6 lõike 1 punktis c) (vastav punkt on ka GDPR-is, art 5 lg 1 p c)) sätestatu näeb ette vastutavale töötlejale tingimusteta kohustuse, ehk kohustuse töödelda isikuandmeid nii palju, kui on see vajalik eesmärgi saavutamiseks[84]. Samuti

[81] (EL) 2016/679. Põhjenduspunkt nr 50.
[82] *Ibid.*
[83] (EL) 2016/679. Põhjenduspunkt nr 39.
[84] EKo C-139/01. *Joseph Lauermann vs Österreichizcher Radfunk.* ECLI:EU:C:2003:294. P 100.

tähendab isikuandmete töötlemise minimaalsuse printsiip seda, et isikuandmeid tuleb töödelda vaid juhul, kui eesmärki, milleks isikuandmeid töödeldakse, ei ole võimalik muud moodi saavutada[85]. Isikuandmete asjakohasust on analüüsinud ELK, leides, et algselt seaduslik täpsete andmete töötlemine võib aja möödudes sattuda direktiiviga[86] vastuollu, kui andmeid ei ole enam tarvis eesmärkidel, milleks neid algselt töödeldi[87]. Eelkõige on tegemist sellise olukorraga, kui andmed ei ole enam adekvaatsed ega asjakohased või kui andmed on neid eesmärke ja möödunud aega arvestades ülemäärased[88].

Rahapesu ja terrorismi rahastamise tõkestamise kontekstis on üsna keeruline ette kujutada, kuidas kohustatud isikud saaksid hoolsusmeetmeid või nende eesmärke täita muul viisil, kui isikuandmeid töödeldes. Seega tuleb krediidiasutustel ning muudel kohustatud isikutel GDPR-i kohaselt järgida, et isikuandmeid töödeldaks ainult nii palju kui on tarvis hoolsusmeetmete täitmiseks. Arvatavasti on isikuandmete töötlemise minimaalsuse printsiipi keeruline järgida, eriti kuna isikuandmete töötlemise minimaalsus eeldab ka seda, et isikuandmeid võib säilitada vaid nii kaua, kuni on täidetud isikuandmete töötlemiseks seatud eesmärk. Selle tagamiseks peab vastutav töötleja määrama kindlad tähtajad, millal isikuandmed kustutatakse, või perioodiliselt üle vaadatakse[89]. See tähendab, et krediidiasutus ise saab kindlaks määrata tähtaja, mille möödumisel vaadatakse uuesti üle isikuandmete töötlemine ning vajadusel kustutatakse ära andmed, mille töötlemine enam vajalik ei ole.

Sellise tähtaja seadmisel ei ole krediidiasutus autori arvates seotud RahaPTS §-s 47 sätestatud andmete säilitamise tähtaegadega. Seadusest tulenevalt peab kohustatud isik säilitama teatud liiki andmeid viis aastat pärast ärisuhte lõppemist, kuid kõigi muude isikuandmete puhul saab krediidiasutus ise otsustada, kui kaua andmeid säilitada. Sellisel juhul tuleb autori arvates lähtuda rangelt isikuandmete töötlemise minimaalsuse printsiibist ning eesmärgi täitmisel tuleb isikuandmed kustutada. GDPR-i põhjenduste kohaselt saab krediidiasutus ise vastutava töötlejana kindlaks määrata tähtajad, millal isikuandmed kustutatakse või millal isikuandmed uuesti üle vaadatakse. Krediidiasutus võib selliste tähtaegade määramisel autori arvates kasutada riskipõhist lähenemist. Kui isik on rahapesu ja terrorismi rahastamise tõkestamise seisukohalt kõrgema riskiga isik (näiteks on isik pärit kõrge riskiga kolmandast riigist, riskitegurite kohta vt lähemalt ptk 1.2.2.) võiks krediidiasutus tihemini selliste klientide andmed

[85] (EL) 2016/679. Põhjenduspunkt nr 39.
[86] Direktiivi all on silmas peetud enne GDPR-i kohaldumist kehtinud Euroopa Parlamendi ja nõukogu direktiivi 95/46/EÜ.
[87] EKo C-131/12, *Costeja Conzalez vs Google Spain and Google,* ECLI:EU:C:2014:317. p 92.
[88] *Ibid.*
[89] (EL) 2016/679. Põhjenduspunkt nr 39.

üle vaadata ning madalama riskiga isikute kohta kogutud andmed pikema perioodi järel üle vaadata. Näiteks kui isik on pärit Korea Rahvademokraatlikust Vabariigist, mis on suure riskiga kolmas riik, kellest lähtub pidev ja märkimisväärne rahapesu ja terrorismi rahastamise oht[90], võiks krediidiasutused andmeid kontrollida ning uuendada iga kolme kuu tagant. Samas, kui isik on pärit EL liikmesriigist, võiks piisata, kui isikuandmeid uuendatakse kahe aasta tagant. Selline näide illustreerib vaid autori poolt soovitatavat riskipõhist lähenemist ka isikuandmete kaitse seisukohalt ning välja pakutud perioodid ei pruugi olla vajalikud. Ka selliste ajaperioodide kindlaks määramisel saab krediidiasutus arvestada oma riskiisu.

Rahapesu ja terrorismi rahastamise tõkestamise tugevdatud hoolsusmeetmete kohaldamise peatükis (1.2.2.) on autor muuhulgas kirjeldanud ka riikliku taustaga isikute suhtes hoolsusmeetmete kohaldamist. Neljanda rahapesu direktiivi artikli 22 kohaselt on riikliku taustaga isikute puhul kohustatud isikutel, sh krediidiasutustel, võimalus kohaldada tugevdatud hoolsusmeetmeid riikliku taustaga isiku, tema pereliikmete või lähedaste kaastöötajate suhtes vähemalt 12 kuud pärast riikliku taustaga isiku ametiaja lõppemist, kuid direktiiv ei sätesta maksimaalset perioodi, millal võib sellise isiku suhtes kohaldada tugevdatud hoolsusmeetmeid. Teoreetiliselt oleks sellisel juhul võimalik krediidiasutusel koguda endise riikliku taustaga isiku ning tema pereliikmete ja lähedaste kaastöötajate suhtes andmeid koguda ja töödelda kuni ärisuhte lõppemiseni. Samuti sätestab neljas rahapesu direktiiv, et hoolsusmeetmete kohaldamine pärast riikliku taustaga isiku ametiaja lõppemist, sõltub konkreetse kohustatud isiku riskihinnangust. Seega, teoreetiliselt võiks krediidiasutus koguda rohkelt isikuandmeid selliste isikute kohta põhjendusega, et nende riskihinnangust tulenevalt tuleks konkreetse isiku suhtes kohaldada lisaks üldistele hoolsusmeetmetele, veel tugevdatud hoolsusmeetmeid.

Autori arvates ei tohiks selline tegutsemine olla isikuandmete kaitse vaatest korrektne ega lubatav, kuna läheb vastuollu isikuandmete töötlemise minimaalsuse printsiibiga. Isikuandmeid võib säilitada vaid nii kaua, kui see on vajalik eesmärgi täitmiseks, seejärel tuleb need jäädavalt kustutada. Kui krediidiasutus soovib pärast 12 kuud riikliku taustaga isiku staatuse lõppemist endiselt kohaldada tugevdatud hoolsusmeetmeid, tuleb seda põhjendada, kuna selliselt riivatakse isiku õigust tema isikuandmete kaitsele intensiivselt. Autori arvates ei oleks sellisel juhul piisav pelgalt põhjendus, et konkreetse endisest riikliku taustaga isikust tuleneb rahapesu ja terrorismi rahastamise alane oht. Krediidiasutus peaks ära näitama konkreetsed potentsiaalsed ohuallikad, mis annaksid võimaluse rohkem andmeid koguda. FATF on oma

[90] Korea Rahvademokraatlik Vabariik on nr 1 suure riskiga kolmas riik Euroopa Komisjoni delegeeritud määruse (EL) 2016/1675 (viide nr 45) kohaselt.

suunistes riikliku taustaga isikute kohta[91] kirja pannud nö ''punased lipukesed'', mis võivad endast kujutada olukordi millal võib olla põhjus kahelda, et riikliku taustaga isik on seotud rahapesu või terrorismi rahastamisega. Sellised olukorrad võivad olla näiteks, kui riikliku taustaga isik on üritanud varjata oma identiteeti, riikliku taustaga isiku käitumine on ebatavaline (isik teeb päringuid kohustatud isiku rahapesu ja terrorismi rahastamise poliitika kohta või ei ole eriti aldis esitama vajalikku informatsiooni), riikliku taustaga isiku osalused äriühingutes, äriühingute tegevusvaldkonnad, millega riikliku taustaga isik seotud on (relvatööstus, pangandus jms), milliseid tooteid või kanaleid riikliku taustaga isik kasutab või millisest geograafilisest piirkonnast on riikliku taustaga isik pärit[92]. Autori arvates võib krediidiasutus koguda riikliku taustaga isiku ning tema pereliikmete või lähedaste kaastöötajate kohta andmeid vaid juhul, kui krediidiasutus suudab tõendada, et esineb tegelik oht (näiteks viidates FATF-i poolt kirjeldatud olukordadele) rahapesu ja terrorismi rahastamiseks, kuna vastupidine läheks vastuollu isikuandmete töötlemise minimaalsuse printsiibiga. Tuleb siiski silmas pidada, et FATFi poolt kirja pandud olukorrad võivad ainult viidata olukorrale, kus riikliku taustaga isiku suhtes võib pikemat aega kohaldada hoolsusmeetmeid, mistõttu ei ole autori arvates õigustatud andmete edasine töötlus põhjusel, et riikliku taustaga isik või tema lähikondne teeb krediidiasutusele päringuid nende rahapesu ja terrorismi rahastamise tõkestamise poliitika kohta. Sellised päringud ei tõenda autori arvates piisavalt seda, et selline isik kujutab endast niivõrd suurt ohtu, et tema isikuandmeid peaks edaspidi töötlema. Seega peaks krediidiasutuste tõendamiskoormis üsna kõrge, kuna isiku õigust tema andmete kaitsele riivatakse intensiivselt.

Autori arvates on krediidiasutustel rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmeid kohaldades üsna lihtne minna vastuollu isikuandmete töötlemise minimaalsuse põhimõttega. Kuna rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmete sisuks on tegelikult võimalikult palju andmete kogumine (hoolsusmeetmete sisust ja liikidest on autor kirjutanud esimeses peatükis) ja trahvid hoolsusmeetmete täitmata jätmisel või puudulikul täitmisel on suured, on krediidiasutuste huvi kindlasti tagada, et hoolsusmeetmeid kohaselt täidetakse. Siiski tuleb arvesse võtta ka seda asjaolu, et ka isikuandmete kaitse õiguste rikkumisel on üsna rasked tagajärjed. Nimelt on GDPR-i artikli 83 lg 5 kohaselt võimalik määrata vastutavale töötlejale rahaline trahv, mille suurus on kuni 20 000 000 eurot või ettevõtja puhul kuni 4% tema eelneva majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt kumb summa on suurem. Samad trahvimäärad on sätestatud ka IKS §-s 65 ning §-s 66. Rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmete

[91] FATF Guidance. Politically exposed persons (recommendations 12 and 22) (viide nr 18). 2013.
[92] *Ibid.* Annex 1. Lk 29-34.

kohaldamata jätmisel või mittekohasel täitmisel on samuti kehtestatud suured trahvimäärad. Rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmete rakendamise rikkumisega kaasneb krediidiasutusele ka mainekahju, mis võib rahalisest karistusest olla veelgi karmim. Kuna krediidiasutuste ja tema klientide vahelises suhtes on oluline just usaldusväärsus, siis krediidiasutuse ebapiisav tegevus rahapesu ja terrorismi rahastamise vastases võitluses võib kahjustada krediidiasutuse mainet ja vähendada klientide usaldust, mille tõttu omakorda võivad kliendid lahkuda ning krediidiasutus kaotab teatud määral oma turuosa. Seega tuleb isikutel, kes on rahapesu neljanda direktiivi mõistes kohustatud isikud ning samas ka vastutavad isikuandmete töötlejad GDPR-i mõistes, leida tasakaal, kuidas koguda piisavalt palju andmeid, et täita rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmeid ning kuidas koguda ja säilitada piisavalt vähe andmeid, et tagada isikuandmete töötlemise minimaalsus.

2.2.3. Isikuandmete töötlemise õigsuse printsiip

GDPR-i artikli 5 lg 1 p d) kohaselt tagatakse isikuandmete töötlemisel, et isikuandmed on õiged ja vajaduse korral ajakohastatud ning et võetakse kõik mõistlikud meetmed, et töötlemise eesmärgi seisukohast ebaõiged isikuandmed kustutataks või parandataks viivitamata (''õigsus'').

Vastutaval töötlejal on kohustus tagada, et isikuandmed, mida töödeldakse on õiged ja ajakohased. Isikuandmete õigsuse nõue ning printsiip on oluline, kuna ebaõigete isikuandmete töötlemine võib viia ebaõige tulemuseni. Eriti oluline on andmete õigsus sellise töötlemise korral, mis on automatiseeritud või koostatakse andmesubjekti kohta profiilianalüüs[93], kuna sellisel juhul töödeldakse isikuandmeid ning tehakse automatiseeritud andmete töötlemise tagajärjel andmesubjekti suhtes mingi otsus. Profiilianalüüsi korral töödeldakse isikuandmeid andmesubjektiga seotud prognoosi tegemiseks, isegi kui andmesubjekti kohta otsust ei tehta.

Automatiseeritud isikuandmete töötlemist kasutatakse muuhulgas panganduse valdkonnas, väiksemate laenude taotlemisel ja väljastamisel. Näiteks kasutab Swedbank AS automatiseeritud isikuandmete töötlemist väikelaenu taotlemisel. Kui Swedbank AS internetipangas täita väikelaenu taotlus, teavitab Swedbank AS, et ''finantstoodete otsuse tegemiseks, töötleb Swedbank Sinu isikuandmeid esitatud taotluse alusel. Otsus taotletava toote

[93] Profiilianalüüs GDPR-i artikli 4 p 4 kohaselt on igasugune isikuandmete automatiseeritud töötlemine, mis hõlmab isikuandmete kasutamise füüsilise isikuga seotud teatavate isiklike aspektide hindamiseks, eelkõige selliste aspektide analüüsimiseks või prognoosimiseks, mis on seotud asjaomase füüsilise isiku töötulemuste, majandusliku olukorra, tervise isiklike eelistuste, huvide, usaldusväärsuse, käitumise, asukoha või liikumisega.

kohta võib olla tehtud automaatselt. Lisaks andmetele, mis on esitatud selles taotluses, hindab Swedbank Sinu krediidivõimekust ja võlgnevusi, töödeldes andmeid välistest registritest.'' Samuti sätestab Swedbank AS ''Kliendiandmete töötlemise põhimõtete'' punkt 4, et Swedbank AS kasutab profiilianalüüsi mh automatiseeritud otsuste tegemisel, näiteks laenuvõime hindamisel ning muuhulgas tehingute kontrollimiseks pettusega võitlemisel[94]. Sarnaselt on AS LHV Pank oma ''Kliendiandmete töötlemise põhimõtete'' punktis 6.1 sätestanud, et automatiseeritud otsuseid kasutatakse maksejõuetuse tõenäosuse hindamisel ning teatud krediidiotsuste tegemisel (nt järelmaks, väikelaen)[95]. AS LHV Pank ning Swedbank AS näitel selgub, et automatiseeritud isikuandmete töötlust kohaldatakse selliste toodete puhul, mis oma olemuselt on väiksema riskiga muuhulgas rahapesu ja terrorismi rahastamise hoolsusmeetmete vaatenurgast. Väikelaenu taotlemisel ei ole laenusummad niivõrd suured[96], võrreldes teiste laenutoodetega, et ühel näites ühel korral väikelaenu taotledes, tekitaks see koheselt kahtlusi. Siiski peab krediidiasutus rahapesu ja terrorismi rahastamise hoolsusmeetmete kohaldamise kohustusest tulenevalt aru saama sellise tehingu eesmärgist.

AS LHV Pank on töötleb kliendi krediidivõimelisuse hindamisel ja krediidiriski juhtimisel: isiklikke andmeid, pereandmeid, kutsetegevuse andmeid, finantsandmeid, süüteoandmeid, võlaandmeid, maksekonto andmeid, tagatiste andmeid, pensioniandmeid, andmeid seoste kohta kolmandate isikutega, vara päritolu andneid ning maksuandmeid. Suurt osa eelnimetatud andmete liikidest töödeldakse automatiseeritult teatud krediidiotsute tegemisel[97]. Autori arvates on väga oluline, et sellisel juhul oleks krediidiasutusel olemas kõik vajalikud andmed ning veelgi olulisem on, et need andmed oleks õiged ja ajakohased.

Kui klientide isikuandmed, mida krediidiasutus töötleb automatiseeritult, on ebaõiged, on tulemuseks ka ebaõige otsus. Näiteks, kui krediidiasutusel on andmesubjekti kohta teada tema ebaõige alaline elukoht, mis on nt kõrge riskiga kolmandas riigis, siis võib automatiseeritult isikuandmeid töödeldes andmesubjekt saada kehvema krediidivõime hinnangu ning seetõttu ebasoodsamad laenutingimused (kõrgem intress, kõrgem krediidikulukuse määr jne). Juba

[94]Swedbank AS ''Kliendiandmete töötlemise põhimõtted''. Arvutivõrgus: https://www.swedbank.ee/static/pdf/private/home/important/gdpr/Principles_of_processing_Personal_data_EE_EST_01032021.pdf (20.03.2021).
[95] AS LHV Pank ''Kliendiandmete töötlemise põhimõtted''. Arvutivõrgus: https://www.lhv.ee/et/kliendiandmete-tootlemise-pohimotted#profiilianal-s-ja-automatiseeritud-otsuste-tegemine-f-silisest-isikust-klientide-kohta (20.03.2021).
[96] AS LHV Pank pakub väikelaenu summas kuni 10 000 eurot, Swedbank AS pakub väikelaenu summas kuni 20 000 eurot.
[97] AS LHV Pank. ''Kliendiandmete töötlemise põhimõtted'' (viide nr 95). Punkt 3.7.

seetõttu on autori arvates kriitilise tähtsusega, et krediidiasutusel oleks kogutud õiged andmed oma klientide kohta.

Kuna automatiseeritud isikuandmete töötlemisel ei tee andmesubjekti suhtes otsust teine inimene, on GDPR-i artikli 22 lg 1 kohaselt andmesubjektil õigus, et tema kohta ei võetaks vastu otsust, mis põhineb üksnes automatiseeritud töötlusel, sealhulgas profiilianalüüsil, mis toob kaasa teda puudutavaid õiguslikke tagajärgi või avaldab talle märkimisväärset mõju[98]. GDPR-i põhjenduste kohaselt võibki sellise märkimisväärse mõjuga otsus olla näiteks veebipõhine krediiditaotluse tagasilükkamine (põhjenduspunkt 71). Seega on andmesubjektile antud võimalus nõuda, et tema kohta tehtav otsus oleks tehtud teise füüsilise isiku poolt, mitte automatiseeritult.

Selleks, et krediidiasutuste poolt kogutud andmed oleksid ajakohased, tuleb neid teatud perioodi järel uuendada või vähemalt paluda klientidel oma edastatud isikuandmed üle vaadata ning kinnitada uued isikuandmed või kinnitada, et juba olemasolevad isikuandmed on endiselt samad. Andmete uuendamine on oluline ka rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmete kohaldamisel. Eriti juriidiliste isikute puhul, kus võib tegelik kasusaaja vahetuda ning uus kasusaaja võib olla isik, kellega krediidiasutus ei soovi ärisuhet jätkata. Ka andmete õigsuse puhul nagu ka isikuandmete töötlemise minimaalsuse printsiibi kohaselt (vt ptk 2.2.2.), on krediidiasutusel kui vastutaval töötlejal õigus ise määrata kindlaks periood, mille järel klientide isikuandmed üle kontrollitakse. Sellisel juhul võiks kohaldada riskipõhist lähenemist ning kõrgema riskiga klientide osas kontrollida nende isikuandmeid ja nende õigusust tihemini, kui madala riskiga klientide osas, kuid konkreetsed protseduurireeglid kehtestab kohustatud isik ise oma riskihinnangust lähtuvalt. Siinkohal tuleks arvestada lisaks isikuandmete minimaalsuse printsiipi, mida on autor kirjeldanud eelmises alapeatükis. Isikuandmete töötlemise minimaalsuse printsiibi kohaselt tuleb isikuandmed kustutada, kui eesmärk, milleks andmeid koguti on saavutatud. Kui krediidiasutus uuendab oma kliendi suhtes isikuandmeid teatud perioodi järel ning selle tulemusena kogub krediidiasutus uusi andmeid, tuleks vananenud andmed kindlasti kustutada. Isikuandmete kustutamisel tuleb silmas pidada, et kustutamisena ei saa käsitleda isikuandmete arhiveerimist, kuna arhiveerimine on isikuandmete töötlemine[99]. Jäädavalt kustutamisel tuleb andmed hävitada nii, et neid ei oleks võimalik ühegi tehnilise vahendi abil kunagi taastada[100].

[98] (EL) 2016/679. Põhjenduspunkt 71.
[99] Seletuskiri isikuandmete kaitse seaduse eelnõu juurde. Lk 24. Arvutivõrgus: https://www.aki.ee/sites/default/files/dokumendid/reform/iks_sk_21.03.18.pdf (20.03.2021).
[100] *Ibid.*

Seega on väga oluline, et andmed, mida krediidiasutused koguvad ning töötlevad, oleks õiged, vajalikud ning ajakohased. Andmete õigsus annab võimaluse täpsemini hinnata muuhulgas rahapesu ja terrorismi rahastamise riske. Kui krediidiasutused kontrollivad piisavalt tihedalt oma klientide isikuandmeid ning paluvad klientidel isikuandmeid muuta või olemasolevaid kinnitada, aitab see kiiremini märgata mõne kliendi osas riskide suurenemist või vähenemist. Kliendiandmete pidev uuendamine võib autori arvates vähendada ka hoolsusmeetmete kohaldamise rikkumise riski. Järelevalveasutuste poolt jälgitakse eelkõige seda, kas krediidiasutus monitoorib oma kliente piisavalt palju, mis kätkeb endas muuhulgas kliendiandmete uuendamist. Kui krediidiasutus täidab uuendamiskohustust piisavalt tihti ja klient esitab krediidiasutusele tahtlikult ebaõigeid andmeid, laskub vastutus osaliselt ebaõigeid andmeid esitanud kliendile.

Käesolevas peatükis kirjeldatud isikuandmete töötlemise põhimõtted on autori arvates kõige rohkem seotud rahapesu ja terrorismi rahastamise hoolsusmeetmete rakendamisega. See ei tähenda, et ülejäänud isikuandmete töötlemise põhimõtted (seaduslikkus, õiglus, läbipaistvus, säilitamise piirang, usaldusväärsus ja konfidentsiaalsus) oleks vähem olulised.

Konfidentsiaalsus GDPR'i mõistes tähendab seda, et isikuandmeid töödeldakse viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid (art 5 lg 1 p f). Ehk vastutaval töötlejal tuleb tagada, et isikuandmetele ei pääse ligi ükski kolmas isik, kellel ei ole õigust isikuandmeid töödelda. GDPR'i art 23 lg 1 p d) kohaselt võib piirata andmesubjektide õigusi, mis on sätestatud GDPR'i artiklites 12-22 ja artiklis 34, kui piirang austab põhiõiguste ja-vabaduste olemust ning on demokraatlikus ühiskonnas vajalik ja proportsionaalne meede, et tagada süütegude tõkestamine, uurimine või avastamine. Seega kui krediidiasutusel on tarvis edastada andmed näiteks korrakaitseasutustele süüteo uurimiseks, tuleb iga kord kaaluda, kas täiendav andmete töötlemine on proportsionaalne meede ning kas süüteo uurimist saaks läbi viia ilma andmeid edastamata.

Siiski ei ole need ülejäänud põhimõtted autori hinnangul niivõrd märkimisväärsed käesoleva magistritöö raames ning nende kirjeldamine oleks liialt väljunud käesoleva magistritöö skoobist.

3. ÕIGUSLIKUD ALUSED ISIKUANDMETE TÖÖTLEMISEKS KREDIIDASUTUSTEL, RAHAPESU JA TERRORISMI RAHASTAMISE TÕKESTAMISE HOOLSUSMEETMETE RAKENDAMISEL

Käesolevas peatükis analüüsib autor, millised võimalused on krediidiasutustel isikuandmete töötlemiseks, kui nad soovivad ühtlasi rakendada rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmeid.

Esmalt analüüsib autor, kuidas ja millistel alustel tuleb rahapesu direktiivide kohaselt isikuandmeid töödelda. Eelkõige soovib autor leida vastust küsimusele, kas rahapesu direktiivid annavad krediidiasutustele või muudele kohustatud isikutele võimaluse isikuandmeid töödelda laialdasemalt, kui seda võimaldab GDPR või tuleb krediidiasutustel siiski järgida kõiki GDPR-is sätestatud põhimõtteid ning isikuandmete töötlemise aluseid. Samuti analüüsib autor, millistel juhtudel riivatakse isikute õigust isikuandmete kaitsele rohkem.

Juhul kui rahapesu direktiivid ei sätesta erinorme isikuandmete töötlemise osas, analüüsib autor, millistel õiguslikel alustel saavad krediidiasutused isikuandmeid töödelda. Selleks kirjeldab autor GDPR-i artiklis 6 sätestatud isikuandmete töötlemise seaduslikkuse aluseid.

Kui krediidiasutused peavad rahapesu ja terrorismi rahastamise tõkestamiseks isikuandmete töötlemisel järgima GDPR'i, ei ole selge, milliseid andmeid ning millises ulatuses võib neid töödelda. Krediidiasutustel võib sellisel juhul olla väga laialdane tõlgendus GDPR'i sätetest, mille tõttu riivatakse andmesubjektide õigusi kohati väga intensiivselt.

3.1. Isikuandmete töötlemine rahapesu ja terrorismi rahastamise tõkestamise õigusaktide järgi

Rahapesu direktiivide rakendamise teatavate aspektidega kaasneb isikuandmete töötlemine, mis peaks olema lubatud vaid juhul, kui austatakse täielikult põhiõigusi ning vaid direktiivis sätestatud eesmärkidel ja vaid selliste toimingute jaoks, mida nõuab direktiiv. Sellisteks toiminguteks on kliendi suhtes hoolsusmeetmete rakendamine, kahtlaste ning tavapäratute tehingute seire, kahtlaste tehingute uurimine ja nendest teatamine pädevatele asutustele, juriidilise isiku tegeliku kasusaaja või riikliku taustaga isiku tuvastamine.[101]

[101] (EL) 2015/849. Põhjenduspunkt nr 43.

Neljanda rahapesu direktiivi põhjenduspunkti nr 65 kohaselt austatakse direktiivis põhiõigusi ja järgitakse hartas[102] tunnustatud põhimõtteid, muuhulgas eelkõige õigust era- ja perekonnaelu austamisele, õigust isikuandmete kaitsele, ettevõtlusvabadust, õigust kohtulikule arutamisele ja süütuse presumptsioonile. Sellest nähtub, et ka rahapesu ja terrorismi rahastamise vastasel võitlemisel tuleb arvestada isikute põhiõigustega. Isegi kui rahapesu neljanda direktiivi eesmärk on finantssektori läbipaistvamaks muutmine ning kuritegeliku päritoluga raha ringlusesse laskmise takistamine, ei saa seda teha teiste põhiõiguste arvelt. Kuivõrd austatakse neljanda rahapesu direktiiviga ka hartas tunnustatud põhimõtteid, võib väita, et isikuandmete töötlemisel tuleb silmas pidada eelkõige isikuandmete töötlemise eesmärgipärasuse põhimõtet, kuna seda sätestab konkreetselt harta artikkel 8 lg 2, kuid autori arvates tuleb arvestada ka kõikide teiste isikuandmete töötlemise printsiipidega. Lisaks tuleb silmas pidada, et harta artikkel 52 sätestab proportsionaalsuse põhimõtte kõikide põhiõiguste riive osas, mistõttu peab ka isikuandmete kaitse õiguse riive olema eesmärgi suhtes proportsionaalne. Kohustatud isikute poolt isikuandmete töötlemine peaks piirduma vaid sellise töötlemisega, mis on vajalik direktiividest tulenevate nõuete täitmiseks[103]. Isikuandmeid ei tohi töödelda sellisel viisil, mis pole rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmete kohaldamisega seotud ning rangelt tuleks keelata isikuandmete täiendav töötlemine ärilistel eesmärkidel[104].

Isikuandmete kaitset reguleerib neljandas rahapesu direktiivis viies peatükk. Artikkel 40 näeb ette, et kohustatud isikud säilitavad siseriikliku õigusega kooskõlas sellised dokumendid ja teabe, mida rahapesu andmebürood või muud pädevad asutused saavad kasutada võimaliku rahapesu või terrorismi rahastamise tõkestamiseks, avastamiseks ja uurimiseks. Nagu RahaPTS §-s 47, on ka direktiivis kirjas, et hoolsuskohustuse täitmisel kogutud dokumente säilitatakse viis aastat pärast ärisuhte lõppu või juhusliku tehingu tegemist.

Pärast viit aastat on kohustatud isikutel kohustus saadud andmed kustutada, kui siseriiklikus õiguses ei ole sätestatud teisiti. Direktiiv annab liikmesriikidele võimaluse otsustada, millistel juhtudel võivad kohustatud isikud säilitada andmeid kauem kui viis aastat (art 40). Liikmesriigid võivad pikemaajalist andmete säilitamist lubada vaid pärast seda, kui on põhjalikult hinnatud sellise säilitamise vajalikkust ja proportsionaalsust ning pikem andmete säilitamise tähtaeg on õigustatud rahapesu või terrorismi rahastamise tõkestamise, avastamise

[102] Harta all on peetud silmas Euroopa Liidu Põhiõiguste Hartat (viide nr 8).
[103] (EL) 2015/849. Põhjenduspunkt nr 43.
[104] *Ibid.*

või uurimise seisukohast. Siiski ei või selline pikemaajaline periood olla pikem kui viis lisa aastat. Seega on kohustatud isikutel direktiivi järgi võimalik kokku säilitada sellised andmeid 10 aastat, olenevalt liikmesriigi otsustusest. RahaPTS § 47 lg 7 näeb ette, et pädeva järelevalveasutuse ettekirjutuse alusel võib rahapesu või terrorismi rahastamise tõkestamise, avastamise või uurimise seisukohast olulisi andmeid säilitada kauem, kuid mitte rohkem kui viis aastat pärast esmase tähtaja möödumist. Järelikult saab Eestis samuti andmeid säilitada kokku 10 aastat, kuid säilitatavad andmed peavad olema olulised. Millised on olulised andmed, ei ole kuskil defineeritud, seega tuleb iga kaasuse puhul eraldi hinnata, kas andmed, mida säilitati, olid olulised süüteo uurimiseks või avastamiseks.

Selline lisa-viieaastane periood andmete säilitamiseks võib anda liikmesriikidele liialt suure kaalutlusruumi, mis tekitab küsimusi andmekaitse õiguse osas küsimusi. Rahapesu direktiivid oleksid võinud anda täpsemad suunised, millal oleks andmete säilitamise tungivalt periood vajalik[105]. Praeguse sõnastuse juures on antud liikmesriikidele vaba võimalus otsustada millisel juhul lisa ajaperioodi kohaldada võib ning kui liikmesriik siseriiklikult seda rangemalt ei reguleeri, võib andmeid säilitada pea iga kord ning andmetega tuleb miskit ette võtta vaid siis, kui andmesubjekt seda nõuab. Tihti ei hooma andmesubjektid milliseid ning mis ulatuses isikuandmeid nende kohta erinevad vastutavad töötlejad on kogunud ning seetõttu ei pruugi andmesubjekt märgata õigusrikkumist. Samuti oleks autori hinnangul ebaõiglane ning ebaproportsionaalne panna selline koormis andmesubjektidele, ka sellepärast, et andmesubjektid ei hooma kõiki nende kohta kogutud isikuandmeid. See tähendaks, et andmesubjektid peaksid kõikide asutuste poole pöörduma, et nende andmed kustutataks. Eestis on seadusandja viieaastase lisaperioodi puhul täpsustanud, et andmeid tohib üle viie aasta säilitada vaid siis, kui selleks on olemas pädeva järelevalveasutuse ettekirjutus (RahaPTS § 47 lg 7). Krediidiasutuste puhul peaks selliseks pädevaks asutuseks olema Finantsinspektsioon.

Direktiivi artikli 41 lg 1 esimese lause kohaselt kohaldatakse muuhulgas rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmete rakendamisel toimuvale isikuandmete töötlemisele direktiivi 95/46/EÜ, nagu see on siseriiklikku õigusesse üle võetud. Kui isikuandmeid direktiivile vastavalt töötlevad Euroopa komisjon või Euroopa järelevalveasutused, kohaldatakse määrust (EÜ) nr 45/2001. Seega tuleb isikuandmete kaitse direktiivi kohaldada

[105] Mitsilegas,V., Vavoula, N., The evolving EU anti-money laundering regime. Challanges for Fundamental Rights and the Rule of Law. Maastricht Journal of European and Comparative Law. Issue 1/2016. Lk 22. Arvutivõrgus: https://heinonline-org.ezproxy.utlib.ut.ee/HOL/Page?collection=journals&handle=hein.journals/maastje23&id=278&men_tab=srchresults (20.04.2021).

kõigil kohustatud isikutel, kes on loetletud rahapesu neljanda direktiivi artiklis 2 lg-s 1. Kuna neljas rahapesu direktiiv võeti vastu enne GDPR-i vastuvõtmist, on direktiivis viidatud enne GDPR-i kehtinud isikuandmete kaitse direktiivile.

Rahapesu viienda direktiivi põhjenduspunkti nr 38 kohaselt tuleb direktiivi raames toimuvale isikuandmete töötlemisele kohaldada Euroopa Parlamendi ja nõukogu määrust (EL) 2016/679 ning sellest tuleb füüsilisi isikuid, kelle isikuandmeid hoitakse tegelikult kasu saavate omanikena riiklikes registrites, asjakohaselt teavitada.

Rahapesu neljas kui ka viies direktiiv sätestavad konkreetselt, et kui isikuandmeid töödeldakse seoses rahapesu ja terrorismi rahastamise tõkestamisega, tuleb järgida isikuandmete kaitse üldmääruses sätestatut.

3.1.1. Isikuandmete kaitse õiguse suuremad riived rahapesu direktiivide kohaselt

Autor on esimeses peatükis selgitanud erinevaid rahapesu ja terrorismi rahastamise tõkestamiseks kohaldatavaid hoolsusmeetmeid. Tugevdatud hoolsusmeetmete sisust tulenevalt kogutakse ja töödeldakse just tugevdatud hoolsusmeetmete kohaldamisel kõige rohkem isikuandmeid, kuna selliste isikute suhtes on kõige suurem risk rahapesu või terrorismi rahastamisega. Autor on eelmises peatükis selgitanud, kuidas riikliku taustaga isikute suhtes on rahapesu neljanda direktiivi alusel võimalik tugevdatud hoolsusmeetmeid kohaldada ka pärast isiku ametiaja lõppemist, kuid seda saab teha vaid siis, kui see on vajalik ja põhjendatud.

Lisaks riikliku taustaga isikutele, riivatakse autori arvates keskmisest rohkem ka tegelike kasusaajate õigusi isikuandmete kaitsele, kuna tegelike kasusaajate andmetele on kõige suuremal ringil isikutel ligipääs.

Neljanda rahapesu direktiivi artikkel 30 lg 3 kohustab liikmesriike tagama, et tegelike kasusaajate andmed hoitakse iga liikmesriigi keskregistris. Eesti puhul tähendab see äriregistrit. Sama sätte neljanda lõike kohaselt peab olema selline teave piisav, täpne ja ajakohastatud. Teave kasusaavate isikute kohta on igasugustel asjaoludel kättesaadav:

a) pädevatele asutustele ja rahapesu andmebüroole ilma piiranguteta;
b) kohustatud isikutele, kui klientide suhtes rakendatakse hoolsusmeetmeid;
c) kõigile isikutele ja organisatsioonidele, kes suudavad tõendada õigustatud huvi.

Punktis c) sätestatud isikutel ja organisatsioonidel on juurdepääs vähemalt tegeliku kasusaaja nime, sünnikuu ja -aasta, kodakondsuse, elukohariigi ning tema majandustegevuse valdkonna kohta. Direktiiv lisab, et juurdepääs sellisele informatsioonile peab olema kooskõlas andmekaitsenormidega ning sellisele informatsioonile juurdepääsuks võib rakendada tasu maksmise või veebipõhise registreerimise kohustust, kuid nõutav tasu ei või ületada teabele juurdepääsu lubamise halduskulusid (art 30 lg 5). Rahapesu andmebüroole ning pädevatele asutustele piiranguta juurdepääsu andmine on oluline, kuna selle kaudu saavad need asutused efektiivsemalt uurimist ning järelevalvet läbi viia. Kohustatud isikutele juurdepääsu andmine on samuti vajalik, kuna kohustatud isikuid, eriti krediidiasutusi kasutatakse enim rahapesuks või terrorismi rahastamiseks ning juhul, kui kohustatud isikutel puuduks kasu saava omaniku andmetele juurdepääs, oleks äärmiselt keeruline tuvastada, kas kliendi poolt edastatud teave tegelikult kasu saava omaniku kohta on õige. Võimalus oleks sellisel juhul nõuda kliendilt tegelikult kasu saava omaniku kohta teavet pädeva isiku poolt tõendatud kujul (notariaalselt tõestatud dokument, välisriigi pädeva isiku poolt tõestatud dokument). Kolmandatele isikutele juurdepääsu andmiseks, tuleb neil tõendada õigustatud huvi sellise teabe osas. Selleks võib olla huvi seoses rahapesu ja terrorismi rahastamise ja nendega seotud eelkuritegudega, nagu korruptsioon, maksukuriteod ja kelmus[106]. Seega peab selline õigustatud huvi olema suunatud just rahapesu ja terrorismi rahastamise tõkestamisele. Kui isikul või organisatsioonil (mitte kohustatud isik direktiivi mõistes) on huvi teha tehing või luua ärisuhe ning isik või organisatsioon soovib ise kohaldada omaalgatuslikult hoolsusmeetmeid oma tehingupartneri osas, ei pruugi selline huvi autori arvates olla piisav, et tegelikult kasu saava isiku andmetele ligipääs saada, kuna keskregistrisse kasu saavate omanike kogutavate andmete eesmärk on aidata takistada rahapesu ja terrorismi rahastamist.

Neljanda rahapesu direktiivi kohaselt sai üldsus tegelike kasusaajate kohta teavet vaid sellisel juhul, kui neil on põhjendatud huvi ning vajadus sellistele andmetele juurdepääsu saada. Viienda rahapesu direktiiviga laiendati sellist üldsuse ringi veel rohkem. Viienda rahapesu direktiivi punktis 15) on sätestatud, et neljanda rahapesu direktiivi artikli 30 lg 5 asendatakse selliselt, et liikmesriigid tagavad, et igal juhul on tegelikult kasu saava omaniku kohta käiv teave kättesaadav:

a) pädevatele asutustele ja rahapesu andmebüroodele ilma piiranguteta;
b) kohustatud isikutele, kui nad rakendavad oma klientide suhtes hoolsusmeetmeid;
c) üldsusele.

[106] (EL) 2015/849. Põhjenduspunkt nr 14.

Punktis c) sätestatud isikutel peab juurdepääs olema vähemalt sellisele teabele tegelikult kasu saava omaniku kohta nagu: nimi, sünnikuu ja -aasta, elukohariik, kodakondsus ning kasu saamisega seotud majandustegevus ning selle ulatus. Seega ei sätesta viies rahapesu direktiiv täiendavat eeldust, millal üldsus peaks saama juurdepääsu kasu saavate omanike andmetele, nadu see oli sätestatud neljandas rahapesu direktiivis.

Nii neljas kui viies rahapesu direktiiv sätestab tegelikult kasu saavate isikute kaitsmiseks võimaliku erandi. Nimelt on liikmesriigil võimalus neljanda rahapesu direktiivi art 30 lg 9 (viienda rahapesu direktiivi punkt 15 g)) kohaselt kehtestada, et tegeliku kasusaaja andmetele antakse vaid osaline juurdepääs või ei anta üldse juurdepääsu (kohustatud isikutele ning üldsusele), kui selle tulemusena tekiks tegelikult kasu saava omaniku suhtes ebaproportsionaalselt suur kelmuse, inimröövi, šantažeerimise, väljapressimise, ahistamise, vägivalla või ähvardamise oht, või kui tegelikult kasu saav omanik on alaealine või muul viisil juriidiliselt teovõimetu. Sellisel juhul tuleb neid erandlikke asjaolusid põhjalikult analüüsida ja kaaluda ning tuleb ka tagada, et erandi tegemise otsus oleks halduskorras läbivaadatav ning tagataks tõhus õiguskaitsevahend. Käesoleval hetkel on Euroopa Liidu kohtus eelotsuse taotlus, kus soovitakse muuhulgas teada, kas GDPR-iga on vastuolus olukord, kus üldsusele tehakse kättesaadavaks teave tegelikult kasu saava omaniku kohta, kuid isikuandmete töötlemise eesmärgist lähtudes ei kohaldada mingit piirangut nende isikuandmete ulatusele ja nendele juurdepääsemise osas[107].

Autori arvates on viienda rahapesu direktiivi puhul antud üldsusele liiga lihtne juurdepääs tegelikult kasu saavate omanike andmetele ning tegelikult kasu saavad omanikud saavad end ja oma andmeid kaitsta vaid siis, kui neid ähvardab otsene oht nende elule või varale. Selline lähenemine riivab autori arvates ebaproportsionaalselt tegelikult kasu saavate isikute põhiõigusi, eriti kuna neljanda rahapesu direktiivi artikli 30 lg 8 kohaselt tuleb tagada, et kohustatud isikud ei toetu tegelikult kasu saava isiku tuvastamisel vaid sellisele keskregistrile ehk sellistel keskregistritel ei ole tegelikkuses õigustloovat jõudu. Seega ei ole nõutav, et tegelikult kasu saava isiku andmed, mis on sellistes keskregistrites, oleksid tõesed ning seal võivad andmed olla vananenud. Samuti ei ole autori arvates piisav kaitsemeede see, et liikmesriigid võivad otsustada, et tegelikult kasu saavate omanike kohta tehakse informatsioon teatavaks vaid juhul, kui selleks on vaja veebis registreeruda ja maksta tasu, mis ei ületa

[107] C–601/20, *Sovim SA.*

informatsiooni kättesaadavaks tegemise halduskulusid, kaasaarvatud registri hooldus- ja arengukulusid. Kuna sellise tasu eesmärk ei ole rikastuda, ei saa need tasud olla piisavalt kõrged, et takistaksid üldsusel juurdepääsu taotlemast.

Autori arvates võib liiga kergelt üldsusele sellise teabe kättesaadavaks tegemine minna vastuollu isikuandmete töötlemise eesmärgipärasuse printsiibiga, kuna sellisel juhul pole võimalik kontrollida, kes tegelikult sellistest keskregistritest andmeid kogub ja neid töötleb. Samuti ei ole võimalik andmesubjekti teavitada eesmärkidest, milleks sellistest avalikest registritest andmeid üldsegi kogutakse ega pole võimalik aru saada millistel eesmärkidel või kes üldse isikuandmeid kogub. Tuleb arvesse võtta ka seda, et tegelikult kasu saav omanik ei edasta oma andmeid sellistesse keskregistritesse andmeid vabatahtlikult, vaid selleks kohustab teda seadus, või muu õigusakt. Sellisel juhul tuleks autori arvates tagada tegelikult kasu saavate omanike õigus nende isikuandmete kaitsele, mida autori hinnangul käesoleval hetkel kehtiv viies rahapesu direktiiv ei taga.

Üldsusele tegeliku kasusaaja andmetele juurdepääsu andmise kohta on Euroopa Andmekaitseinspektor võtnud seisukoha, et selline ebakindlus, kui laiendatakse andmete töötlemise eesmärki niivõrd, et selleks ei ole enam esmane rahapesu vastane eesmärk, vähendab andmete kaitse kaitsemeetmeid, nagu proportsionaalsus isikuandmete töötlemise ning selle töötlemise eesmärgi vahel[108]. Euroopa Andmekaitseinspektori selgituste järgi on nende suurim mure selles, et ükskõik missugune isikuandmete töötlemine peab olema seaduslikul, konkreetsel ja arusaadaval eesmärgil ja seotud vajalikkuse ning proportsionaalsusega, samuti peab isikuandmete töötleja olema tuvastatav ning tema tegevus peab vastama isikuandmete kaitse reeglitele[109]. Seega riivatakse tegelikult kasu saavate omanike õigusi nende andmete kaitsele rohkem, kuna nende andmetele on ligipääs üldsusele, kes ei pea enam põhjendama, miks neil selliseid andmeid tarvis on.

GDPR-i kohaselt on üheks andmesubjekti õiguseks õigus teada milliseid andmed tema kohta kogutakse ja töödeldakse. GDPR-i artikkel 12 lg 1 sätestab, et vastutav töötleja võtab asjakohased meetmed, et teavitada andmesubjekti tema kohta kogutud andmetest. Seda tuleb teha kokkuvõtlikult, arusaadavalt ning lihtsasti kättesaadavas vormis. Sama põhimõte oli sätestatud ka enne GDPR-i vastu võtmist kehtinud isikuandmete kaitse direktiivis 95/46/EÜ. See eeldab ka seda, et andmesubjekti teavitatakse asjaolust, et tema isikuandmeid töödeldakse.

[108] European Data Protection Supervisor. Opinion 02.02.2017 (viide nr 76). Lk 9.
[109] *Ibid.*

Kui isikuandmeid töödeldakse rahapesu direktiivide raames, piiratakse andmesubjekti õigust saada enda kohta kogutavate andmete kohta teavet, kuna andmesubjekti juurdepääs kahtlase ja ebatavalise tehinguga seotud teabele pärsib rahapesu ja terrorismi rahastamise vastase võitluse tulemuslikkust[110]. Sellise piirangu jaoks on GDPR-i artiklis 23 sätestatud, et andmesubjekti õigusi, sealhulgas andmetele juurdepääsu õigust võib piirata, kui selline piirang austab põhiõiguste ja -vabaduste olemust ning on demokraatialikus ühiskonnas vajalik ja proportsionaalne meede, et tagada muuhulgas süütegude tõkestamine, uurimine avastamine või nende eest vastutusele võtmine, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmine ja nende ennetamine. Seega juhul, kui rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmete rakendamisel tuvastab kohustatud isik ebatavalise või kahtlase tehingu, või kohustatud isik täiendavalt andmeid töödelda andmesubjekti teavitamata. Vastasel juhul võib isik asuda end või tehtud tehinguid ning varasid varjama hakata, mis tõepoolest takistaks oluliselt selliste kahtlaste tegevuste uurimist ning nendest teavitamist. Siiski ei saa andmesubjekti õigust piirata kergekäeliselt ning see peab olema vajalik ning proportsionaalne. Autori arvates tuleks kohaldada riskipõhist lähenemist, ehk kui esineb suurem risk, et isik või tehing on seotud rahapesu või terrorismi rahastamisega, võiks andmesubjektile anda vähem teavet ning vastupidi, väiksema riskiga andmesubjektile tuleks anda rohkem teavet. Sellist piirangut peab krediidiasutus muidugi põhjendama ning tõendama. Kui krediidiasutus suudab põhjendada, et kliendist A tulenev rahapesu või terrorismi rahastamise risk on oluliselt suurem kui kliendist B tulenev risk, siis võib olla põhjendatud kliendile A vähesema teabe esitamise. Riskipõhine lähenemine aitaks siinkohal andmesubjekti õiguse riivet vähendada, sest kui krediidiasutuse hinnangul ei tulene kliendist suurt ohtu, võib talle suuremas osas teavet anda, millega riivataksegi isiku õigust andmetele juurdepääsuks.

Eeltoodust nähtub, et rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmeid tuleb kohaldada kooskõlas isikuandmete kaitse üldmäärusega ning kohustatud isikud peavad arvestama kõikide isikuandmete töötlemise põhimõtetega. Eelnevalt on autor kirjeldanud riikliku taustaga isikute isikuandmete töötlemist pärast nende ametiaja lõppemist ja kuidas on piisava põhjuse olemasolul võimalik säilitada riikliku taustaga isikute isikuandmeid kuni 10 aastat pärast ametiaja lõppemist. Lisaks riikliku taustaga isikutele piiratakse õigust isikuandmete kaitsele autori arvates enim tegelikult kasusaavate omanike suhtes. Nende isikuandmetele on juurdepääs kõige suuremal ringil isikutel, mis autori arvates on liialt tegelike

[110] (EL) 2015/849. Põhjenduspunkt nr 46.

kasusaajate eraellu sekkumine ning ei taga rahapesu ja terrorismi rahastamise tõkestamise eesmärki, mistõttu on see autori arvates vastuolus ka isikuandmete töötlemise eesmärgipärasuse põhimõttega. Lisaks piiratakse kõikide isikute juurdepääsuõigust oma andmetele. Sellise piirangu vajadus on tõenäoliselt vajalik ja proportsionaalne, kuna vastupidisel juhul oleks keeruline süütegude tõkestamine või uurimine. Kui kahtlase tehingu teinud isik saab koheselt teada, et tema andmeid täiendavalt töödeldakse ning tehtud tehinguid uuritakse täiendavalt, on isikul koheselt võimalik vajalikke asjaolusid varjama asuda.

Järgnevalt analüüsib autor, millistel õiguslikel alustel on võimalik isikuandmeid töödelda, kui kohustatud isikud rakendavad rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmeid.

3.2. Isikuandmete töötlemise alused rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmete rakendamisel

GDPR-i artikkel 6 sätestab isikuandmete töötlemise seaduslikkuse alused. Lg 1 kohaselt on isikuandmete töötlemine seaduslik ainult juhul, kui on täidetud vähemalt üks järgmistest tingimustest ning sellisel määral, nagu see tingimus on täidetud:

a) andmesubjekt on andnud nõusoleku töödelda oma isikuandmeid ühel või mitmel konkreetsel eesmärgil;
b) isikuandmete töötlemine on vajalik andmesubjekti osalusel sõlmitud lepingu täitmiseks või lepingu sõlmimisele eelnevate meetmete võtmiseks vastavalt andmesubjekti taotlusele;
c) isikuandmete töötlemine on vajalik vastutava töötleja juriidilise kohustuse täitmiseks;
d) isikuandmete töötlemine on vajalik andmesubjekti või mõne muu füüsilise isiku eluliste huvide kaitsmiseks;
e) isikuandmete töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks;
f) isikuandmete töötlemine on vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral, välja arvatud juhul, kui sellise huvi kaaluvad üles andmesubjekti huvid või põhiõigused ja -vabadused, mille nimel tuleb kaitsta isikuandmeid, eriti kui andmesubjektiks on laps.

Rahapesu ja terrorismi rahastamise tõkestamise kontekstis on arutori arvates kõige asjakohasemad alused vastutava töötleja juriidilise kohustuse täitmine, avalikes huvides oleva ülesande täitmine ning isikuandmete töötlemine vastutava töötleja õigustatud huvi korral.

Enne, kui kohustatud isikud ärisuhte loovad, ehk hakkavad muuhulgas töötlema klientide isikuandmeid, tuleb neljanda rahapesu direktiivi artikli 41 lg 3 kohaselt uutele klientidele esitada direktiivi 95/46/EÜ artiklis 10 sätestatud teave. Samasisuline säte on GDPR-i artikkel 13, ehk teave, mis tuleb andmesubjektile esitada juhul, kui andmed on kogutud andmesubjektilt. Artikli 13 lg 1 kohaselt tuleb andmete saamise ajal (rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmete kontekstis on see enne ärisuhte loomist) andmesubjektile esitada vastutava töötleja nimi ning kui kohaldatav, siis vastutava töötleja esindaja nimi ja kontaktandmed, asjakohasel juhul andmekaitseametniku kontaktandmed, isikuandmete töötlemise eesmärk ja õiguslik alus, kui isikuandmete töötlemine põhineb vastutava töötleja õigustatud huvil, siis teave selliste õigustatud huvide kohta, asjakohasel juhul teave isikuandmete vastuvõtjate või vastuvõtjate kategooriate kohta ning kui asjakohane, siis teave selle kohta, kas vastutav töötleja kavatseb isikuandmed edastada kolmandale riigile või rahvusvahelisele organisatsioonile. Lisaks tuleb andmesubjekti teavitada isikuandmete säilitamise ajavahemikust ning muuhulgas teavitada andmesubjekti selle kohta, et tal on õigus taotleda juursepääsu enda andmetele ning õigus nõuda nende parandamist või kustutamist või töötlemise piiramist. Kui vastutav töötleja kavatseb isikuandmeid edasi töödelda muul eesmärgil, kui algne eesmärk, peab vastutav töötleja seda andmesubjektile teada andma ja teavitama teda nendest täiendavatest eesmärkidest, milleks vastutav töötleja andmeid edaspidi töödelda kavatseb.

Isikuandmeid on alati võimalik töödelda muuhulgas andmesubjekti enda nõusolekul. Sellisel juhul on võimalik vastutaval töötlejal töödelda isikuandmeid nii palju ja sellises ulatuses ning enda seatud eesmärkidel kui andmesubjekt selleks nõusoleku andnud on. Kui andmesubjekt on nõus, et tema isikuandmeid töödeldakse nii ärilistel eesmärkidel kuid samal ajal ka rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmete kohaldamiseks, on see võimalik. Järelikult annab andmesubjekti nõusolek võimaluse laialdaselt isikuandmeid töödelda, kuid andmesubjekti nõusoleku alusel isikuandmete töötlemist on peetud üsna nõrgaks isikuandmete töötlemise aluseks[111].

[111] WP29. Opinion 15/2011 on the definition on consent. 13.07.2011. lk 10. Arvutivõrgus: https://www.pdpjournals.com/docs/88081.pdf (22.03.2021).

Nõusoleku alusel isikuandmete töötlemine võib keeruliseks osutuda pelgalt juba seetõttu, et andmesubjektil on GDPR art 7 lg 3 kohaselt õigus oma nõusolek igal hetkel tagasi võtta ning vastutaval töötlejal pole enam seejärel seaduslikku alust isikuandmeid töödelda, mistõttu tuleb need isikuandmed kustutada, kuna andmesubjektil on GDPR art 17 alusel õigus olla unustatud. Kohane nõusolek peab olema kas kirjalik või suuline, kuid igal juhul konkreetne ning teadlik nõusolek, mistõttu ei saa andmesubjekti vaikimist nõusolekuks pidada[112].

Samuti peab vastutav töötleja suutma tõendada, et andmesubjekt on nõusoleku andnud vabatahtlikult. Nõusoleku tõendamise kohustus hõlmab ka seda, et vastutav töötleja peab tõendama, et tal oli andmesubjekti nõusolek ka selliseks andmetöötluseks, mille ulatus algselt ei olnud nii lai[113]. Järelikult tuleb enne nõusoleku saamist andmesubjektile selgitada, et tema isikuandmeid võidakse töödelda erinevatel eesmärkidel ning erinevatel ajahetkedel. Arvestades, et nõusoleku üheks tingimuseks on andmesubjekti vabatahtlikkus, on selgelt näha seadusandja tahe, mille kohaselt ei tohiks andmesubjektid olla survestatud nõusolekut andma[114]. Näiteks ei saa nõusolekut vabatahtlikuks lugeda, kui andmesubjekt ja vastutav töötleja on selgelt ebavõrdses seisus, eelkõige juhul, kui vastutav töötleja on avaliku sektori asutus ja näiteks, kui teenuse osutamine on pandud sõltuma nõusolekust[115]. Seega ei saa näiteks krediidiasutus nõuda, et andmesubjekt oleks nõus laialdase isikuandmete töötlemisega ning vastasel juhul ei ole krediidiasutus nõus pakkuma andmesubjektile makseteenust või ei ole nõus pangakontot avama. Sellisel juhul oleks andmesubjekt väga ebavõrdses olukorras ning oleks sunnitud oma andmete töötlemiseks nõusoleku andma või talle ei võimaldata tänapäeva ühiskonnas väga vajalikke teenuseid. Tõenäoliselt ei haaku praktiline elu sellise käsitlusega. Juhul, kui klient ei ole nõus laialdase andmetöötlusega, on krediidiasutusel võimalus keelduda ärisuhte loomisest, kas RahaPTS-s sätestatu alusel (krediidiasutus ei ole võimeline täitma hoolsusmeetmeid) või krediidiasutuste seaduse[116] § 89 lg-s 9 sätestatu alusel, ehk krediidiasutusel on õigus otsustada, kellele teenust pakkuda. Kui andmesubjekt leiab, et temaga ärisuhte loomisest on ebaseaduslikult keeldutud, tuleks pöörduda kohtusse. Tõenäoliselt ei soovi ükski andmesubjekt läbida kohtuvaidlust selleks, et krediidiasutuses nt arvelduskontot avada. Seega seniks, kuni ükski andmesubjekt sellist krediidiasutuse tegevust ei vaidlusta, on krediidiasutustel võimalus praktikat jätkata.

[112] (EL) 2016/679. Põhjenduspunkt nr 32.
[113] (EL) 2016/679. Pühjenduspunkt nr 42.
[114] Kelleher, D., Murray, K. EU Data Protection Law. Bloomsbury Professional: 2018. lk 155.
[115] (EL) 2016/679. Põhjenduspunkt nr 43.
[116] RT I, 04.01.2021, 33

Samuti tuleb arvestada, et nõusoleku tagasivõtmise korral peab vastutaval töötlejal olemas olema välja töötatud süsteem, mis tagab, et andmesubjekti nõusoleku tagasivõtmisel andmetöötlus lõpetatakse[117].

Kuna andmesubjekti nõusolek oma isikuandmete töötlemiseks võib kujuneda üsna problemaatiliseks, on autori arvates oluline rahapesu ja terrorismi rahastamise tõkestamise eesmärgil töödelda isikuandmeid teistel alustel. Järgnevalt kirjeldabki autor, millistel juhtudel ning millised kriteeriumid tuleb täita, et isikuandmeid töödelda avalikes huvides oleva ülesande täimiseks, juriidilise kohustuse täitmiseks või õigustatud huvi korral.

3.2.1. Isikuandmete töötlemine avalikes huvides oleva ülesande täitmiseks

Kui isikuandmete töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks, peaks töötlemise alus olema sätestatud liidu või liikmesriigi õigusaktis. Iga üksiku isikuandmete töötlemise toimingu reguleerimise jaoks ei ole vaja eraldi õigusakti, vaid võib piisata sellisest õigusaktist, mille alusel saab teha mitu isikuandmete töötlemise toimingut, kui töötlemine on avalikes huvides oleva ülesande täitmiseks vajalik. Sellisel juhul peab sellises õigusaktis olema kirjas olema isikuandmete töötlemise eesmärk, et andmesubjektil oleks võimalik konkreetselt aru saada, miks tema isikuandmeid töödeldakse. Samuti peab liikmesriik oma siseriikliku õigusaktiga ära reguleerima, kes on sellised isikud, kellel on lubatud isikuandmeid töödelda avalikes huvides oleva ülesande täitmiseks, ehk kas vastutavad töötlejad peaks olema avaliku sektori asutused või muud avalik-õiguslikud juriidilised isikud või eraõiguslikud juriidilised isikud[118].

Nii neljas kui ka viies rahapesu direktiiv sätestavad, et direktiivi alusel toimuv isikuandmete töötlemine rahapesu ja terrorismi rahastamise tõkestamise eesmärgil on käsitletav avaliku huvi küsimusena GDPR-i mõistes (art 43). Seega, kui kohustatud isikud töötlevad isikuandmeid rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmeid kohaldades, on üheks isikuandmete töötlemise õiguslikuks aluseks GDPR artikkel 6 lg 1 p e) ehk isikuandmete töötlemine avalikes huvides oleva ülesande täitmiseks. Sellest nähtub, et rahapesu ning terrorismi rahastamise vastane võitlus on käsitletav avaliku huvi küsimusena. Seda, et terrorismi vastane võitlus on üldist huvi pakkuv Euroopa Liidu eesmärk ja julgeolekut tagav

[117] Kelleher. D., Murray, K. Lk 155.
[118] (EL) 2016/679. Põhjenduspunkr nt 45.

eesmärk, on kinnitanud ka ELK[119]. Terrorismi rahastamise takistamine on avaliku huvi küsimus, kuna kuritegelike rahavoogude ringlusesse sattumise takistamine ei saa olla vaid ühe või mõne liikmesriigi või mõne institutsiooni või organisatsiooni eesmärk, vaid terrorismi rahastamine on ohuks tervele maailmale ning seda tuleb takistada ülemaailmselt. Kuna rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmete kohaldamine on isikuandmete kaitse vaatest isikuandmete töötlemine avalikes huvides oleva ülesande täitmine, tuleks liikmesriikidel õigusaktiga reguleerida, kes on sellised isikud, kellel on luba isikuandmeid sellel alusel töödelda. RahaPTS § 48 lg-st 2 võib järeldada, et isikuandmete töötlemise õigus on kõigil kohustatud isikutel, kes on loetletud sama seaduse §-s 2.

Kui isikuandmeid töödeldakse avalikes huvides oleva ülesande täitmiseks, ehk käesoleval juhul rahapesu ja terrorismi rahastamise tõkestamiseks, tuleb rangelt lähtuda isikuandmete töötlemise eesmärgipärasuse ning minimaalsuse põhimõttest. Seda sätestab ka RahaPTS § 48 lg 2, mille kohaselt võib kohustatud isik seaduse rakendamisel kogutud isikuandmeid töödelda üksnes rahapesu ja terrorismi rahastamise tõkestamise eesmärgil. Seega on keelatud igasugune andmete töötlemine, mis ei täida seda eesmärki.

Andmesubjektil peaks siiski olema võimalus esitada vastuväiteid või vaidlustada oma isikuandmete töötlemine ka siis, kui tema isikuandmeid töödeldakse avalikes huvides oleva ülesande täitmiseks[120]. Sellisel juhul on tõendamiskoormis pandud vastutavale töötlejale, kes peab tõendama, et tema mõjuvad õigustatud huvid kaaluvad üles andmesubjekti huvid või põhiõigused ja -vabadused[121]. Rahapesu ja terrorismi rahastamise kontekstis peaks kohustatud isik seega tõendama, et isik, kelle andmeid töödeldakse, kujutab endast niivõrd suurt ohtu finantssektorile, et isikuandmete töötlemine on äärmiselt vajalik muuhulgas ka süüteo uurimiseks või avastamiseks. Tõenäoliselt pärsib andmesubjekti selline taotlus süüteo uurimist pärast selle avastamist. Kui andmesubjekt esitab vastutavale töötlejale vastuväite oma isikuandmete töötlemise osas ning vastutav töötleja sellist taotlust ei rahulda, võib see andmesubjektile anda indikatsiooni, et tema suhtes võib käimas olla uurimine ning kui selline andmesubjekt ka tegelikult rahapesu või terrorismi rahastamisega seotud on, võib ta asuda oma vara, selle päriolu või muid olulisi asjaolusid varjama. Ehk teisisõnu on oht, et oma andmete töötlemisele vastuväite esitamisel saab andmesubjekt teada tema kohta käivast uurimisest, mis põhjuse olemasolul uurimist takistab. Juhul, kui vastutav töötleja keeldub taotluse

[119] C – 293/12 ja C – 594/12 *Digital Rights Ireland Ltd vs Minister for Communications.*
[120] (EL) 2016/679. Põhjenduspunkt nr 69.
[121] *Ibid.*

rahuldamisest, kuid andmesubjekt on veendunud, et tema andmeid ebaseaduslikult töödeldakse on võimalik pöörduda kohtusse ning nõuda õigusvastase tegevuse keelamist võlaõigusseaduse (edaspidi VÕS)[122] § 1055 lg 1, § 1043 ning § 1045 lg 1 p 7 alusel. VÕS § 1055 lg 1 üheks eelduseks on kostja õigusvastane käitumine, milleks isikuandmete töötlemise puhul võib olla VÕS § 1045 lg 1 p-s 7 sätestatu ehk seadusest tuleneva kohustuse rikkumine. Riigikohus on selgitanud, et VÕS § 1045 lg 1 p 7 mõttes on kaitsenormid ka IKS-i sätted[123]. Seega, kui vastutav töötleja rikub isikuandmete töötlemisega seotud norme, on selline tegevus käsitletav õigusvastase tegevusena VÕS § 1045 lg 1 p 7 mõistes. Kui vastutav töötleja ei põhjenda piisavalt, miks andmetöötlus vajalik on, võib kohus andmetöötluse keelata. On võimalik, et vastutavatele töötlejatele on andmetöötluse lõpetamiseks taotlusi tehtud, kuid sellist kaasust kohtupraktikas veel ei nähtu.

3.2.2. Isikuandmete töötlemine vastutava töötleja juriidilise kohustuse täitmiseks

Asjaolu, et rahapesu direktiivid sätestavad konkreetse aluse isikuandmete töötlemiseks, ei tähenda autori arvates seda, et kohustatud isikutel ei oleks võimalust koguda ja töödelda isikuandmeid teistel seaduslikel alustel. GDPR-i artikkel 6 lg 1 sätestab, et isikuandmete töötlemine on seaduslik, kui vähemalt üks nimetatud tingimustest on täidetud. Sellest võib järeldada, et tingimused, mis muudavad isikuandmete töötlemise seaduslikuks, võivad esineda ka kumulatiivselt.

GDPR-i artikkel 6 lg 1 p c) järgi on isikuandmete töötlemine seaduslik, kui isikuandmete töötlemine on vajalik vastutava töötleja juriidilise kohustuse täitmiseks. Säte hõlmab vastutavaid töötlejaid, kes tegutsevad nii avalikus kui erasektoris[124].

Kui isikuandmeid töödeldakse vastutava töötleja juriidilise kohustuse täitmiseks, peaks selline töötlemise alus olema sätestatud Euroopa Liidu või liikmesriigi õigusaktis, mille subjektiks on vastutav töötleja[125]. Iirimaa Andmekaitse komitee[126] seisukoha järgi ei pea juriidiline kohustus alati konkreetselt nõudma sellist isikuandmete töötlemist, mida vastutav töötleja kavatseb teha,

[122] RT I, 04.01.2021, 19.
[123] RKTKo 2-15-16007, p 12.
[124] Euroopa andmekaitseõiguse käsiraamat. 2018 aasta väljaanne. Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu: 2020. lk 151. Arvutivõrgus: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_et.pdf (28.03.2021).
[125] Feiler, L., Forogo,N., Weigl, M., The EU General Data Protection Regulation (GDPR): A Commentary. German Law Publishers: 2018. Lk 84.
[126] Iirimaa Andmekaitse komitee (*The Data Protection Commission*) on Iirimaa iseseisev isikuandmete kaitse järelevalveasutus.

vaid vastutavad töötlejad peavad tagama, et isikuandmete töötlemine üldiselt oleks kooskõlas juriidilise kohustuse täitmisega[127]. Euroopa Liidu või liikmesriigi õigusaktis, millega pannakse kohustus isikuandmeid töödelda, peaks sisaldama ka andmete töötlemise eesmärki ning võiks sisaldada GDPR-i üldtingimusi, millega reguleeritakse isikuandmete töötlemise seaduslikkust, kehtestatakse tingimused vastutava töötleja kindlaksmääramiseks, töötlemisele kuuluvate isikuandmete liik, asjaomased andmesubjektid, üksused, kellele võib andmeid avaldada, eesmärgi piirangud, säilitamise aeg ja muud meetmed seadusliku ja õiglase isikuandmete töötlemise tagamiseks[128]. Samuti tuleks juriidilise kohustuse täitmiseks isikuandmete töötlemisel arvestada sellega, et vastutaval töötlejal ei või sellisel juhul olla valikut, kas täita kohustust või mitte[129].

Rahapesu ja terrorismi rahastamise tõkestamiseks kohaldatavad hoolsusmeetmed, mille raames isikuandmeid töödeldakse, on juriidiline kohustus, mis on sätestatud Euroopa Liidu tasandil rahapesu direktiivides ning direktiivide olemuse tõttu üle võetud liikmesriikide õigusesse. Hoolsusmeetmete rakendamise kohustus on seega väga konkreetne ning samuti väga konkreetse eesmärgiga. Seega saavad kohustatud isikud andmeid töödelda vaid konkreetse juriidilise kohustuse täitmiseks ning väga konkreetsel eesmärgil.

Autori arvates on vastutava töötleja poolt isikuandmete töötlemisel juriidilise kohustuse täitmisel ning avalikes huvides ülesande täitmisel isikuandmete töötlemisel võimalik töödelda sama liiki ning samas ulatuses isikuandmeid. Nagu ka teiste isikuandmete töötlemise aluste puhul, tuleb ka siinkohal rangelt kinni pidada isikuandmete töötlemise eesmärgipärasusest ehk kohustatud isik ei või isikuandmeid töödelda muul eesmärgil, kui rahapesu ja terrorismi rahastamise tõkestamine. Samuti tuleb tagada võimalikult väheste andmete töötlemine, ehk kohustatud isikud vastutavate töötlejatena ei tohi koguda ega töödelda rohkem isikuandmeid, kui neil on tarvis rahapesu ja terrorismi rahastamise tõkestamise eesmärgi saavutamiseks.

[127] Data Protection Commission.Guidance Note: Legal Bases for Processing Personal Data. Detsember 209. Lk 15. Arvutivõrgus: https://www.dataprotection.ie/sites/default/files/uploads/2019-12/Guidance%20on%20Legal%20Bases_Dec19_1.pdf (28.03.2021).
[128] (EL) 2016/679. Põhjenduspunkt nr 45.
[129] Andmekaitse Inspektsiooni juhend, kuidas rakendada isikuandmete kaitse üldmääruse 2016/679 artikkel 6 lõige 1 punktis f sätestatud õigustatud huvi kui andmetöötluse õiguslikku alust. 15.05.2020. Lk 5. Arvutivõrgus: https://www.aki.ee/sites/default/files/dokumendid/oigustatud_huvi_juhend_15052020.pdf (28.03.2021).

3.2.3. Isikuandmete töötlemine vastutava töötleja või kolmanda isiku õigustatud huvi korral

GDPR-i artikkel 6 lg 1 p f) järgi on isikuandmete töötlemine seaduslik, kui isikuandmete töötlemine on vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral, välja arvatud juhul, kui sellise huvi kaaluvad üles andmesubjekti huvid või põhiõigused ja -vabadused, mille nimel tuleb isikuandmeid kaitsta, eriti juhul, kui andmesubjekt on laps. Nagu autor on eelnevalt selgitanud, tuleb õigustatud huvi alusel isikuandmete töötlemisel andmesubjektile selline huvi teatavaks teha enne, kui isikuandmeid töötlema hakatakse (rahapesu neljanda direktiivi artikkel 41 lg 3).

Käesolev magistritöö keskendub vastutavale töötlejale, kes on ühtlasi ka rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmete kohaldamiseks kohustatud isik. Seetõttu ei analüüsi käesolevas alapeatükis autor kolmandate isikute õigustatud huve, vaid piirdub vastutava töötleja poolt isikuandmete töötlemise seaduslikkusega.

Õigustatud huvi on määratlemata õigusmõiste, mistõttu on autori arvates vastutavatel töötlejatel piisava põhjenduse olemasolul, võimalik töödelda üsna laialdaselt ning laialdastel eesmärkidel. Kuna õigustatud huvi mõistet ei ole defineeritud, tuleb selle sisustamiseks pöörduda õiguskirjanduse ning kohtupraktika poole.

Nagu tuleneb GDPR-i sõnastusest, tuleb õigustatud huvi alusel isikuandmete töötlemisel kaaluda vastutava töötleja huvi isikuandmete töötlemise suhtes ning teiselt poolt andmesubjekti põhiõigusi ja -vabadusi. Samuti tuleb võtta arvesse andmesubjekti mõistlikke ootusi, mis põhinevad andmesubjekti ja vastutava töötleja suhtel ning selline õigustatud huvi võib olla olemas kui andmesubjekt on vastutava töötaja klient ja kas andmesubjekt võis andmete kogumise hetkel mõistlikkuse piires eeldada, et neid samu andmeid võidakse töödelda sellisel eesmärgil[130]. Kui andmesubjekt ei saa mõistlikult eeldada isikuandmete edasist töötlust, saab andmesubjekti põhiõigusi ning -vabadusi pidada prevaleerivaks vastutava töötleja õigustatud huvi ees[131]. Selline lähenemine on tuletatav Ameerika Ühendriikide kõrgeima kohtu poolt kehtestatud ''mõistlik ootus privaatsusele'' (ingl *reasonable expectation of privacy*) kontseptsioonist[132]. Kontseptsioonil on kaheastmeline nõue: esmalt peab andmesubjektil olema

[130] (EL) 2016/679. Põhjenduspunkt nr 47.
[131] *Ibid.*
[132] L.Feiler, N. Forgo, M. Weigl. (viide nr 125). Lk 84.

reaalne ootus privaatsusele ning teiseks peab ühiskond olema valmis, et sellist isiku ootust mõistlikuks pidada[133].

GDPR-i artikkel 6 lg 1 p f näeb ette seega kolm tingimust, millal võib isikuandmeid töödelda ning kõik need tingimused peavad olema täidetud:

a. vastutaval töötlejal või andmeid saaval kolmandal isikul või kolmandatel isikutel on õigustatud huvi;
b. isikuandmete töötlemine on vajalik selle õigustatud huvi teostamiseks;
c. vastutava töötleja või andmeid saava kolmanda isiku huve ei kaalu üles kaitstava andmesubjekti põhiõigused ja-vabadused. [134]

''Huvi'' kontseptsioon on üsna sarnane ''eesmärgipärasuse'' kontseptsiooniga, mis on sätestatud isikuandmete kaitse direktiivi artiklis 6 (eesmärgipärasus on sätestatud ka käesoleval hetkel kehtiva GDPR-i artiklis 6). Isikuandmete kaitse kontekstis on ''eesmärk'' spetsiifiline põhjus, miks isikuandmeid töödeldakse, kuid huvi on justkui laiem osalus, mis võib vastutaval töötlejal isikuandmete töötlemisel olla. Vastutava töötleja huvi peab olema piisavalt täpne, et teha nii öelda tasakaalu testi huvi ning andmesubjekti põhiõiguste vahel. Lisaks peab selline huvi olema reaalne ning ajakohane ehk huvi peab olema seotud selle hetke toimingutega või kasuteguritega, mille mõju saab oodata väga lähitulevikus. Ehk selline huvi, mis on liialt ebamäärane, ei ole piisav.[135] Kuivõrd samad põhimõtted, mis kehtisid enne GDPR-i kohaldumist, on ka praegu asjakohased, võib WP29 eeltoodud selgitusi kohaldada ka GDPR-i suhtes. Lisaks peab vastutava töötleja huvi olema õiguspärane, vastasel juhul, kui vastutava töötleja huvi on ebaseaduslik, ei saa ilmselgelt tasakaalu testi kohaldada[136], kuna ühegi andmesubjekti isikuandmeid ei või autori arvates töödelda ebaseaduslikul eesmärgil või huvi olemasolul. Juhul, kui vastutava töötleja huvi on väike ning ei ole veenev, ei tähenda see automaatselt seda, et isikuandmeid õigustatud huvi alusel töödelda ei saaks. Sellisel juhul peab andmesubjekti põhiõiguste riive olema ka vastutava töötleja väiksest huvist ebaolulisem. Huvi võib olla õigustatud kuniks vastutav töötleja saab seda teostada sellisel viisil, mis on kooskõlas isikuandmekaitse ning muude õigusaktidega[137]. WP29 on oma arvamuses kirja pannud

[133] *U.S. Supreme Court. Katz v. United States, 389 U.S. 347 (1967).*
[134] AKI juhend (viide nr 129). Lk 6.
[135] WP29. Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Direcitove 95/46/EC. 09.04.2014. Lk 24. Arvutivõrgus: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (29.03.2021). Sellised eeldused on sätestatud Euroopa Liidu kohtu otsuses C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde vs Rīgas pašvaldības SIA „Rīgas satiksme.* ECLI:EU:C:2017:336. P 28.
[136] *Ibid.*
[137] *Ibid.*

mitteammendava loetelu, millal võib olla vastutataval töötlejal õigustatud huvi isikuandmete töötlemiseks ning sealhulgas on WP29 maininud ka rahapesu tõkestamist[138]. Seega võib rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmete kohaldamiseks kohustatud isikutel, sealhulgas krediidiasutustel, olla õigustatud huvi töödelda isikuandmeid rahapesu tõkestamiseks. Andmekaitse Inspektsioon on oma juhendis selgitanud, et ''õigustatud huvi võib hõlmata isikuandmete töötleja laiemaid huve, nii olulisi kui ka vähemolulisi, st et alles siis, kui selliseid huve hakatakse tasakaalustama andmesubjekti huvide ja põhiõigustega, tuleb kohaldada piiritletumat lähenemisviisi ja sisulisemat analüüsi[139].'' Teisalt tuleb arvesse võtta andmesubjekti põhiõigusi ja -vabadusi. Euroopa Liidu kohus on selgitanud, et andmesubjekti õigused, mida tuleks arvesse võtta on eelkõige harta artiklites 7 ja 8 sätestatud õigused[140].

Selleks, kas vastutava töötleja poolt isikuandmete töötlemine õigustatud huvi alusel on seaduslik, tuleb läbida kolmeastmeline tasakaalustamise test:

I. isikuandmete töötleja huvi ja nende kaalukus;
II. andmesubjekti õigused ja huvid ning nende kaalukus;
III. vastanduvate huvide kaalumine, nende esialgne hinnang, lisaks vajadusel täiendavad kaitsemeetmed ning seejärel lõplik hinnang. [141]

Rahapesu ja terrorismi rahastamise tõkestamise kontekstis oleks autori arvates kohustatud isiku kui vastutava töötleja huvi see, et ta saaks oma juriidilist kohustust täita või aidata tuvastada rahapesu või terrorismi rahastamist. Kohustatud isikutel on kohustus täita rahapesu direktiivides sätestatud eesmärke tagada finantssektori stabiilsus ning takistada kriminaalse taustaga raha ringlusesse sattumist. Kuna rahalised trahvid hoolsusmeetmete kohaldamata jätmisel või mittekohasel täitmisel on suured, on ilmselt kohustatud isiku ehk vastutava töötleja huvi osaliselt ka suuri trahve vältida. Autori hinnangul on kohustatud isikute huvi takistada rahapesu ning terrorismi rahastamise üsna suure kaaluga.

ELK on selgitanud, et andmesubjekti õiguste kaalumisel tuleb arvesse võtta harta artiklis 7 ja 8 sätestatud õigusi[142]. GDPR-i põhjenduspunktis nr 47 on selgitatud, et lisaks andmesubjekti õigustele ja vabadustele, tuleb arvestada ka andmesubjekti huvidega. Erinevalt vastutava

[138] *Ibid.*
[139] AKI juhend (viide nr 129). Lk 6.
[140] C-131/12. *Google Spain SL, Google Inc. vs Agencia de Protección de Datos (AEPD), Mario Costeja González.* ECLI:EU:C:2014:317. Punkt 74 ja seal viidatud kohtupraktika.
[141] AKI juhend (viide nr 129). Lk 6.
[142] *Google Spain SL, Google Inc. vs Agencia de Protección de Datos (AEPD), Mario Costeja González.* Punkt 74.

töötleja huvist, ei ole GDPR-i põhjendustes mainitud andmesubjektide huvi ees terminit ''õigustatud'', mistõttu tuleb arvesse võtta kõiki andmesubjekti huve, mis kaasnevad tema isikuandmete töötlemisega[143]. Asjaolu, et lisaks tuleb arvestada ka andmesubjekti huvidega, annab andmesubjektile autori arvates suurema kaitse, kuna andmesubjekti huvi on määratlemata mõiste. Vastutaval töötlejal tuleb muuhulgas arvestada ka andmesubjekti mõistlikke ootustega oma isikuandmete töötlemisel. Selle puhul tuleb rakendada isikuandmete töötlemise eesmärgipärasuse põhimõtet (vt ptk 2.2.1.).

Kui andmesubjekt on toime pannud kuriteo, siis ei tohiks siiski tema isikuandmeid liiga laialdaselt avalikustada. Näiteks, kui isik on kaubanduskeskusest ehteid või rõivaid varastanud, ei ole põhjendatud tema nimega piltide üles riputamine lähiümbruses. Kannatanu vaatest võib tunduda, et tema huvi võib olla kaalukam, kuid autori arvates on see kaheldav. Siiski võib ebaseadusliku tegevuse puhul andmesubjekti huvi olla väiksema kaaluga kui vastutava töötleja oma, kui tegemist on rahapesu või terrorismi rahastamisega. Näiteks, kui vastutaval töötlejal on teada isik, kes on tuntud terrorirühmitusele hiljuti teinud suures summas annetuse, võib autori arvates vastutav töötleja avaldada sellise isiku isikuandmed üldsusele (nt avaldada isiku nimi ning pilt ajalehes või sotsiaalmeedias) ja neid täiendavalt töödelda. Vahe eelmise näitega on esiteks selles, kui suure kahju on isik oma ebaseadusliku tegevusega põhjustanud ning selles, kui palju isikuid kahtlustatava isikuandmeid näeb. Kuna rahapesu ja terrorismi rahastamise tõkestamine on Euroopa Liidus kui ka väljaspool Euroopa Liitu väga oluline, võib autori arvates terrorismi rahastamises kahtlustatava isiku isikuandmeid töödelda ning avaldada neid ka välismaal. Kuid ka sellisel juhul peab vastutav töötleja enne isikuandmete avaldamist olema täiesti kindel, et avaldatakse õige isiku isikuandmed. Vastasel juhul võib andmesubjektil, kelle andmed ekslikult avaldati, esitada vastutava töötleja vastu kahju hüvitamise nõude. Seega tuleb vastutaval töötlejal iga kord tuvastada, milliseid andmesubjekti põhiõigusi, -vabadusi ja huve arvesse võtta tuleb.

Kui vastutav töötleja on tuvastanud enda huvid ning tuvastanud ka andmesubjekti põhiõigused ja -vabadused, mida isikuandmete töötlemisega riivata võib, tuleb vastutaval töötlejal kaaluda, kumb on olulisem või kas isikuandmete töötlemisel andmesubjektile tekitatav mõju on taotletava eesmärgi suhtes proportsionaalne.

[143] AKI juhend (viide nr 129). Lk 7.

Selleks, kas isikuandmete töötlemisega tekitatav mõju andmesubjektile on taotletava eesmärgi suhtes proportsionaalne, saab kohaldada Eesti õiguspraktikas juurdunud kolmeosalist testi, mille kohaselt on ''abinõu proportsionaalne vaid siis, kui see on püstitatud eesmärgi saavutamiseks sobiv, vajalik ja mõõdukas''[144]. Abinõu on sobiv siis, kui see soodustab piirangu eesmärgi saavutamist. Sellest järeldub, et isikuandmete töötlemine peab olema eesmärgipärane. Kui eesmärki ei ole võimalik saavutada mõnel muul moel, mis oleks andmesubjekti vähem koormavam, võib abinõu pidada vajalikuks ning mõõdukuse hindamisel peab kaaluma ühelt poolt andmesubjekti huve ning nende olulisust (sealhulgas ka andmesubjekti põhiõigusi ja -vabadusi) ning riive ulatust. Teisalt tuleb kaaluda isikuandmete töötlemise eesmärgi tähtsust.[145]

Arvestada tuleb ka isikuandmete liigiga, näiteks kas töödeldakse sensitiivseid isikuandmeid või mitte. Samuti tuleb arvestada, kuidas isikuandmeid töödeldakse ning kui suurele ringile isikutele isikuandmeid avaldatakse. Juhul, kui vastutav töötleja leiab, et isikuandmete töötlemine õigustatud huvi alusel ei läbi tasakaalutesti, võib vastutav töötleja rakendada täiendavaid meetmeid, et andmesubjekti õigusi vähem riivata ning pärast meetmete rakendamist isikuandmete töötlemist uuesti kaaluda. Näiteks on võimalik kasutada pseudonümiseerimist[146], mis autori arvates riivab andmesubjekti õigusi vähem. Tuleb meeles pidada seda, et kaitsemeetmed, mida vastutav töötleja võib täiendavalt kohaldada ei ole andmesubjekti suhtes kaitsemeetmed, mida tuleb vastutaval töötlejal kohaldada seaduse alusel[147]. Sellisel juhul on tegemist vastutava töötleja seadusest tuleneva kohustuse täitmisega ning kui enne seadusest tuleneva kohustuse täitmist leidis vastutav töötleja, et isikuandmete töötlemisest on andmesubjekti õigused olulisemad, ei saa autori arvates seadusest tuleneva kohustuse täitmisel vastutav töötleja asuda seisukohale, et ta on võitnud kasutusele piisavad täiendavad kaitsemeetmed andmesubjekti õiguste kaitseks.

Kui vastutav töötleja on vabatahtlikult kohaldanud kaitsemeetmeid ning uue kaalumise järel leiab, et isikuandmete töötlemine on põhjendatud ja seaduslik, on andmesubjektil siiski õigus GDPR art 21 lg 1 alusel esitada vastuväide tema isikuandmete töötlemisele, mida on töödeldud õigustatud huvi alusel ning nõuda tema isikuandmete töötlemise peatamist ning isikuandmete kustutamist.

[144] AKI juhend (viide nr 129). Lk 7.
[145] AKI juhend (viide nr 129). Lk 8.
[146] GDPR art 4 p 5 järgi on pseudonümiseerimine isikuandmete töötlemine sellisel viisil, et isikuandmeid ei saa enam täiendavat teavet kasutamata seostada konkreetse andmesubjektiga, tingimusel et sellist täiendavat teavet hoitakse eraldi ja andmete tuvastatud või tuvastatava füüsilise isikuga seostamise vältimise tagamiseks võetakse tehnilisi ja korralduslikke meetmeid.
[147] AKI juhend (viide nr 129). Lk 9.

Käesolevas peatükis on autor analüüsinud millisest õigusaktist peavad rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmete kohaldamiseks kohustatud isikud isikuandmete töötlemisel lähtuma. Autor leidis, et rahapesu direktiivid ei sätesta eraldi aluseid isikuandmete töötlemiseks, mistõttu peavad kohustatud isikud lähtuma isikuandmete kaitse üldmääruses sätestatust. Lisaks kirjeldas autor peamisi õiguslikke aluseid, mille alusel isikuandmeid töödelda.

KOKKUVÕTE

Käesolevas magistritöös on autor selgitanud rahapesu ja terrorismi rahastamise vastase võitluse vajalikkust ning tegevusi ja toiminguid, mida isikud, kellel on kõige tõenäolisemalt võimalik mõjutada seda, et kuritegeliku päritoluga raha ei satuks ringlusesse, tegema peavad. Selle tõttu, et Euroopa Liit on rahapesu ja terrorismi rahastamise vastase võitluse viimastel aastatel eredalt esile toonud ning karmistanud reegleid ning seadnud trahvimäärad üsna kõrgeks, on järelevalveasutused järjest rohkem avastanud juhtumeid, kus äriliste eesmärkide saavutamiseks on rahapesu ja terrorismi rahastamise tõkestamise reeglite osas kvaliteeti alla lastud.

Neljandas rahapesu direktiivis on ette nähtud, et rahapesu ja terrorismi rahastamise tõkestamise eesmärgil peab hoolsusmeetmeid rakendama mh krediidiasutus. Magistritöös ongi autor keskendunud krediidiasutuste kui kohustatud isikute tegevusele rahapesu ja terrorismi rahastamise tõkestamisel.

Kohustatud isikute üldine kohustus rahapesu ja terrorismi rahastamise tõkestamisel on teada ning aru saada, kellega tehinguid tehakse või ärisuhet luuakse ning kust pärineb vara, millega soovitakse tehinguid teha. Hoolsuskohustuse rakendamise kohustus tuleneb neljandast rahapesu direktiivist, mis Eestis on üle võetud rahapesu ja terrorismi rahastamise tõkestamise seadusesse (RahaPTS). Sellised kohustused hõlmavad endas kliendi või juhuti tehtavas tehingus osaleva isiku isikusamastuse tuvastamist, esindaja isikusamasuse ning esindusõiguse tuvastamist, tegeliku kasusaaja tuvastamist, teabe hankimisest, kui kohustatud isik ei saa aru juhuti tehtavast toimingust, riikliku taustaga isiku või tema lähikondlase tuvastamist ning ärisuhte seire tegemist (RahaPTS § 20 lg 1).

Eelnimetatud kohustusi tuleb rakendada iga kliendi või juhuti tehtavas tehingus osaleja kohta, ehk need on üldised hoolsusmeetmed, mida tuleb kohaldada, et tegutseda kooskõlas seadusega. Rahapesu neljas direktiiv näeb ette, et teatud juhtudel võib üldiseid hoolsusmeetmeid rakendada lihtsustatult, kuid seda vaid juhul, kui eelnevalt on tuvastatud, et kliendiga seonduv rahapesu või terrorismi rahastamise risk on väike ning riski realiseerumine on pea olematu. Lihtsustatud hoolsusmeetmed võivad endas hõlmata seda, et kliendiandmeid uuendatakse keskmisest harvem. Siiski tuleb krediidiasutustel olla valmis selleks, et kliendi osas, kelle suhtes kohaldati lihtsustatud hoolsusmeetmeid, võib ühel hetkel tekkida kohustus kohaldada tugevamaid hoolsusmeetmeid, kuna kliendi riskitase tõuseb. See võib juhtuda olukorras, kus klient hakkab ootamatult tegema tehinguid suuremates summades või soovib kasutada uusi teenuseid, mis

pole konkreetsele kliendile ega muudele isikutele, kes tegutsevad samas valdkonnas, omapärased. Sellisel juhul tuleb küsida lisateavet, et selgeks teha maksekäitumise muutuse põhjused.

Teatud juhtudel tuleb krediidiasutustel kohaldada tugevdatud hoolsusmeetmeid, ehk tuleb klientidelt küsida veelgi rohkem informatsiooni, et maandada tavapärasemast kõrgemat rahapesu ja terrorismi rahastamise riski. Alati tuleb tugevdatud hoolsusmeetmeid kohaldada näiteks siis, kui tekib kahtlus, et isikusamasuse tuvastamiseks esitatud andmed ei ole tõesed. Tugevdatud hoolsusmeetmeid tuleb kohaldada ka teatud isikute suhtes, kelleks on riikliku taustaga isik ning tema perekond ning lähedane kolleeg. Riikliku taustaga isik on isik, kellele on usaldatud avaliku võimu teostamine ning see toob omakorda kaasa riski sellise staatuse ärakasutamisest, eriti riikides, kus korruptsiooni tase on kõrgem.

Olulisim hoolsusmeede, mida krediidiasutused rakendama peavad on tegeliku kasusaaja tuvastamine, ehk selle isiku tuvastamine, kes ärisuhtest või tehingutest tegelikult kasu saab. Tegelik kasusaaja peab olema tuvastatud füüsilise isiku tasandil, mis võib osutuda keeruliseks, kui ettevõttel on keeruline omandistruktuur, kus äriühingu osanikeks või aktsionärideks on peamiselt teised äriühingud.

Kõikide hoolsusmeetmete kohaldamise kohta tuleb krediidiasutustel RahaPTS § 47 lg 1 kohaselt säilitada dokumentide originaalid või nende koopiad. Dokumente võib säilitada kuni viis aastat pärast ärisuhte lõppemist. Sama sätte lg 7 järgi võib neid dokumente säilitada veel lisaks viis aastat, kuid ainult järelevalveasutuse ettekirjutuse alusel.

Seega on rahapesu ja terrorismi rahastamise tõkestamisel kriitilise tähtsusega andmete kogumine ning nende töötlemine. Liigne andmete kogumine võib sattuda vastuollu isikute õigusega oma isikuandmete kaitsele.

Just isikuandmete kaitse on Euroopa Liidus teine valdkond, mis on viimaste aastate jooksul väga palju populaarsust kogunud. 2016 aastal vastu võetud isikuandmete kaitse üldmäärus, GDPR, ei muutnud juba kehtivaid isikuandmete kaitse printsiipe, kuid muutis need väga aktuaalseks.

Magistritöö teises peatükis ongi autor selgitanud isikuandmete kaitse õigust, selle määratletust õigusaktides ning peamisi põhimõtteid isikuandmete töötlemisel.

Isikuandmete mõiste on üsna lai, hõlmates kõikvõimalikke andmeid, mille abil on võimalik füüsilist isikut tuvastada. Olgu selleks isiku nimi, sünniaeg, isikukood või isiku foto, helisalvestis või sõrmejälg. Samuti on isikuandmete töötlemise definitsioon väga lai. Nimelt on isikuandmete töötlemine iga toiming, mida tehakse isikuandmetega. Seega saab eeltoodust järeldada, et toimingud, mida teevad krediidiasutused, kui nad kohaldavad rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmeid, kujutavad endast tegelikult suures ulatuses isikuandmete töötlemist. Seega on rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmete rakendamiseks kohustustatud isikud ühtlasi vastutavad isikuandmete töötlejad GDPR'i mõistes.

Isikuandmete töötlemisel tuleb arvestada kõikide printsiipidega, mis on GDPR'i artiklisse 5 kirja pandud. Autor valis kuuest printsiibist välja kolm ning kirjeldas neid lähemalt. Need printsiibid, mis autori arvates on rahapesu ja terrorismi rahastamise tõkestamise vaatenurgast eriti olulised, on eesmärgi piirang, andmete töötlemise minimaalsuse ning õigsuse printsiip. Autor on selgitanud nende printsiipide sisu ning seotust rahapesu ja terrorismi rahastamise tõkestamise hoolsusmeetmete kohaldamisega.

Kolmandas peatükis on autor püüdnud välja selgitada, milline on õiguslik raamistik isikuandmete töötlemisel, kui isikuandmeid töödeldakse rahapesu ja terrorismi rahastamise tõkestamiseks. Enne magistritöö kirjutamist eeldas autor, et rahapesu direktiivid näevad ette erialused isikuandmete töötlemiseks, mis võimaldab isikuandmeid töödelda laialdasemalt, kui seda lubab GDPR.

Rahapesu neljanda ning viienda direktiivi kohaselt tuleb isikuandmete töötlemisel juhinduda vaid GDPR'is sätestatust ning erialuseid isikuandmete töötlemiseks rahapesu direktiividest ei nähtu. Seega tuleb ka krediidiasutustel järgida kõiki reegleid, mis tulenevad GDPR'ist, isegi siis, kui nad töötlevad isikuandmeid rahapesu ja terrorismi rahastamise tõkestamise eesmärgil.

Kuna isikuandmete töötlemisel tuleb järgida isikuandmete kaitse üldmääruses sätestatut, kirjeldas autor nelja seaduslikku alust, mida võiks kasutada isikuandmete töötlemise alusena, kui täidetakse rahapesu ja terrorismi rahastamise tõkestamise hoolsuskohustusi. Rahapesu neljanda ja viienda direktiivi järgi töödeldakse isikuandmeid rahapesu ja terrorismi rahastamise tõkestamise hoolsuskohustusi rakendades avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks, mis on GDPR'i artikli 6 lg 1 p-s e) sätestatud

alus isikuandmete töötlemiseks. Lisaks sellele alusele analüüsis autor, kas isikuandmeid saaks töödelda ka vastutava töötleja juriidilise kohustuse täitmiseks või vastutava töötleja õigustatud huvi korral (GDPR art 6 lg 1 p-d c) ning f)) ning mis on sellise töötlemise eeldused.

Magistritöö kirjutamise käigus selgus, et isikuandmete kaitse õiguse ning rahapesu ja terrorismi rahastamise tõkestamise puhul põrkuvad kaks olulist põhimõtet: andmete minimaalne töötlemine isikuandmete kaitse vaatenurgast ning võimalikult suure hulga andmete töötlemine rahapesu ja terrorismi rahastamise tõkestamise vaatenurgast. Kehtiva õiguse kohaselt ei ole rahapesu ja terrorismi rahastamise tõkestamise eesmärk ülimuslik isikuandmete kaitse õigusest, kuivõrd isikuandmete töötlemisel rahapesu ja terrorismi rahastamise tõkestamiseks, tuleb täielikult järgida andmekaitse reegleid ning tagada, et kõikide andmesubjektide eraellu ei sekkutaks ülemäära. Konkreetsed juhud, mil isikuandmete maht ja laad, mida töödeldakse rahapesu ja terrorismi rahastamise tõkestamiseks, on ebaproportsionaalselt suur ning rikub isikute õigusi oma andmete kaitsele, jääb tulevikus kohtupraktika selgitada.

Infringements of right to privacy in the course of due diligence measures to prevent money laundering and terrorist financing and legal basis of precessing personal data by credit institutions

In this Master's thesis the author has clarified the importance of combat against money laundering and terrorist financing and what credit institutions can do to stop the flow of money obtained from criminal activities to society. Because of that the fact that the European Union, in recent years, has brought up the importance of anti money laundering (AML) and counter terrorist financing (CTF) and set very high penalty levels, the supervisory authorities have detected quite a lot cases where the AML and CTF standards have not been met.

The fourth AML directive has set out that credit institutions, among else institutions have to implement the due diligence measures while onboarding a client and during the business relationship. The thesis focuses on the action of credit institutions while implementing due diligence measures.

The general duty is to understand with whom the transactions are made and where are the assets from, that are used to complete the transaction. The duty to imply the due diligence measures comes from the fourth AML directive, in Estonia the directive has been adopted to the Money Laundering and Terrorist Financing Prevention Act. The due diligence measures include identifying the client and its representative, as well as gather more information from the client if the credit institution does not understand the transaction and the purpose of it. Also the due diligence measures have to be implied if the client is a politically exposed person (PEP) or its close family member or close colleague.

According to the fourth AML directive, when a credit institution finds that there is a smaller risk with a client, it can imply simplified due diligence measures. Simplified measures may include that the client's data will be updated more rarely. But the credit institutions have to be careful, if they detect unusual behaviour, they have to imply more due diligence measures. This may happen if a client starts to make more transactions or the value of the transactions are higher than usual. In this case the credit institution have to gather more information to find out what is the reason of this kind of unusual behaviour.

In some cases the credit institutions have to imply enhanced due diligence measures, which means that the business relationship have to be monitored even more frequently. Enhanced due

diligence measures have to be implied if the credit institution has doubts that the information provided by the client, is not true or when the client is a PEP or a close person to PEP.

The most important due diligence measure that the credit institutions have to imply is detecting the beneficial owner (BO) of a company. Beneficial owner is a natural person and detecting a BO can be difficult when a company is owned by lots of other companies and a natural person cannot be found. All the documents gathered during the due diligence have to be stored for five years. If the supervisory authority allows, the documents can be stored extra five years.

So it is very important to collect and process data to be successful in the combat against money laundering and terrorist financing. But when the credit institutions collect too much data, they can be incompatible with the privacy and data protection regulations.

Data protection, alongside AML ang CTF, is very important subject in the European Union. The General Data Protection Regulation (GDPR), which was adopted in 2016, made the principles of data processing very relevant. In the second chapter, author has explained the right to personal data, its definition in different regulations and the most relevant principles of data processing when it comes to AML and CTF.

The definition of personal data is very broad, it contains all data by which a natural person might be detected. Personal data can be a persons name, date of birth, photo or biometrical data. The definition of processing data is also very broad, including all activity that contains personal data. Therefor it can be said that due diligence measures that the credit institutions imply, mean processing personal data. When processing personal data, the credit institutions must comply with the GDPR and have to take into account all the principles in the GDPR. Author picked out three principles of data protection that are the most relevant while applying the due diligence measures: purpose limitation, data minimisation, and accuracy. Author clarified these principles and brought out problems regarding data minimisation principle. The data minimisation principle means that personal data must be collected and processed minimum. But the AML and CTF due diligence measures are successful if a credit institution has lots of data. So the credit institution have to try to balance these two principles.

In the third chapter author tried to find out whether the AML directives set out an independent ground for processing personal data or the credit institutions have to take account all the principles and grounds of processing personal data, according to the GDPR. During writing this

thesis, the author found out that the credit institutions must fully comply with GDPR, while processing personal data and the AML directives do not set out an independent ground for processing personal data while applying due diligence measures.

Since the credit institutions must comply with GDPR while processing personal data for due diligence, author described four grounds for processing personal data. The fourth AML directive sets out that while processing data during due diligence, it would mean that the credit institution processes personal data to perform a task carried out in the public interest or in the exercise of official authority vested in the controller (GDPR article 6 1(e)). In the authors opinion, this does not have to be the only ground for processing data while applying due diligence measures. For that, the author described three other grounds for processing personal data: the data subject's consent, processing personal data for compliance with a legal obligation to which the controller is subject and processing personal data for the purposes of legitimate interest pursued by the controller where such interests are overridden by the interest of fundamental rights and freedoms of the data subject which require protection of personal data.

As a result of writing this thesis, the author found out that while applying due diligence measures to combat money laundering and terrorist financing there is a conflict with principles of processing personal data. While applying the due diligence measures the credit institutions must collect lot of data, but on the other hand, on of the most important principle of data protection, is data minimisation, which means that personal data must be processed as little as possible. Since not one is more important than the other, the credit institutions must be very careful that they will not infringe the right to personal data. Since there are no case-law yet about the conflict of these two principles, the type of personal data and how much personal data can be processed without infringing the data subject's rights to their privacy, will be defined by courts.

KASUTATUD KIRJANDUS

1. De Vido, S., Anti-Money Laundering Measures versus European Union Fundamental Freedoms and Human Rights in the Recent Jurisprudence of the European Court of Human Rights and the European Court of Justice. German Law Journal: 2016. lk 1271 – 1293. Arvutivõrgus: https://heinonline-org.ezproxy.utlib.ut.ee/HOL/Page?collection=journals&handle=hein.journals/germlajo16&id=1307&men_tab=srchresults (23.04.2021).
2. Euroopa andmekaitseõiguse käsiraamat. 2018 aasta väljaanne. Euroopa Liidu Põhiõiguste Amet ja Euroopa Nõukogu: 2020. Arvutivõrgus: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_et.pdf (28.03.2021).
3. Feiler, L., Forogo,N., Weigl, M., The EU General Data Protection Regulation (GDPR): A Commentary. German Law Publishers: 2018.
4. Kelleher, D., Murray, K. EU Data Protection Law. Bloomsbury Professional: 2018.
5. Madise, Ü. PSK – Eesti Vabariigi põhiseadus. Komm vlj. 5. Tallinn: Juura 2020. Arvutivõrgus: https://pohiseadus.ee (15.03.2021).
6. Mitsilegas,V., Vavoula, N., The evolving EU anti-money laundering regime. Challanges for Fundamental Rights and the Rule of Law. Maastricht Journal of European and Comparative Law. Issue 1/2016. Arvutivõrgus: https://heinonline-org.ezproxy.utlib.ut.ee/HOL/Page?collection=journals&handle=hein.journals/maastje23&id=278&men_tab=srchresults (20.04.2021).
7. Sinclari, D (koost.), Fratangelo, P, Formisani, R, Tonnara, P, Zaccagna, A. The New Anti-Money Laundering Law, First Perspectives on the 4th European Union Directive. Edited by Domenico Sinclari. Palgrave Macmillan, 2016.
8. Tibar, I. Tähelepanekuid uue rahapesu ja terrorismi rahastamise tõkestamise seaduse jõustumisega seoses – Juridica 2018/1.

KASUTATUD NORMATIIVALLIKAD

9. Eesti Vabariigi põhiseadus – RT I, 15.05.2015, 2.
10. Euroopa Inimõiguste ja Põhivabaduste Kaitse Konventsioon – RT II 2010, 14, 54.
11. Euroopa Liidu Põhiõiguste harta.

12. Euroopa Parlamendi ja nõukogu direktiiv (EL) 2015/849, 20. mai 2015, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist ning millega muudetakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 648/2012 ja tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2005/60/EÜ ja komisjoni direktiiv 2006/70/EÜ (rahapesu neljas direktiiv) – ELT L 141.
13. Euroopa Parlamendi ja Nõukogu direktiiv (EL) 2018/843, millega muudetakse direktiivi (EL) 2015/849, mis käsitleb finantssüsteemi rahapesu või terrorismi rahastamise eesmärgil kasutamise tõkestamist, ning millega muudetakse direktiive 2009/138/EÜ ja 2013/36/EL (viies rahapesu direktiiv) – ELT L 156.
14. Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ, 24. oktoober 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – ELTL L 281.
15. Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27.aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) – ELT L 119.
16. Isikuandmete kaitse seadus – RT I, 04.01.2019, 11.
17. Isikut tõendavate dokumentide seadus – RT I, 31.01.2020, 15.
18. Komisjoni delegeeritud määrus (EL) 2016/1675, 14.07.2016, millega täiendatakse Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/849, määrates kindlaks suure riskiga kolmandad riigis, kus esineb strateegilisi puudusi. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32016R1675&from=ET .
19. Krediidiasutuste seadus – RT I, 04.01.2021, 33.
20. Rahandusministri 27.09.2020 määrus. Loetelu Eesti ametikohtadest, mille täitjaid loetakse riikliku taustaga isikuteks – RT I, 24.09.2020, 4.
21. Rahapesu ja terrorismi rahastamise tõkestamise seadus. - RT I, 21.11.2020, 13.
22. Äriseadustik – RT I, 04.01.2021, 46.

KASUTATUD KOHTUPRAKTIKA

23. EIKo 30562/04, *S. and Marper v. the United Kingdom.*
24. EIKo 44599/98, *Bensaid v. the United Kingdom.*
25. EKo C-131/12, *Costeja Conzalez vs Google Spain and Google,* ECLI:EU:C:2014:317.
26. EKo C-139/01. *Joseph Lauermann vs Österreichizcher Radfunk.* ECLI:EU:C:2003:294.
27. EKo C-203/15, *Tele2 Sverige AB vs Post-och teletyrelsen.* ECLI:EU:C:2016:970.

28. EKo C-601/20 *SOVIM SA vs Luxembourg Business Registers,* Eelotsusetaotlus.
29. EKo liidetud kohtuasjad C – 293/12 ja C – 594/12 *Digital Rights Ireland Ltd vs Minister for Communications jt,* ECLI:EU:C:2014:238.
30. EKo liidetud kohtuasjad C-92/09 ja C-93/09 *Volker und Markus Schenke GbR ja Hartmut Eifert vs Land Hessen*, ECLI:EU:C:2010:662.
31. RKHKm 3-19-1672.
32. RKHKo 3-3-1-3-12.
33. RKPJKo 3-4-1-6-01.
34. RKPJKo 5-19-38.
35. RKTKo 2-15-16007.

KASUTATUD MUUD ALLIKAD

36. Andmekaitse Inspektsiooni juhend, kuidas rakendada isikuandmete kaitse üldmääruse 2016/679 artikkel 6 lõige 1 punktis f sätestatud õigustatud huvi kui andmetöötluse õiguslikku alust. 15.05.2020. Arvutivõrgus: https://www.aki.ee/sites/default/files/dokumendid/oigustatud_huvi_juhend_15052020.pdf (28.03.2021).
37. AS LHV Pank. ''Kliendiandmete töötlemise põhimõtted''. Arvutivõrgus: https://www.lhv.ee/et/kliendiandmete-tootlemise-pohimotted#profiilianal-s-ja-automatiseeritud-otsuste-tegemine-f-silisest-isikust-klientide-kohta (20.03.2021).
38. Basel Committee on Banking Supervision. Customer due diligence for banks. October 2001.
39. Data Protection Commission. Guidance Note: Legal Bases for Processing Personal Data. Arvutivõrgus: https://www.dataprotection.ie/sites/default/files/uploads/2019-12/Guidance%20on%20Legal%20Bases_Dec19_1.pdf (28.03.2021).
40. Euroopa Pangandusjärelevalve. Direktiivi (EL) 2015/849 artikli 17 ja artikli 18 lõike 4 alusel koostatud ühissuunised, milles käsitletakse kliendi suhtes rakendatavaid lihtsustatud ja tugevdatud hoolsusmeetmeid ning tegureid, mida krediidi- ja finantseerimisasutused peaksid arvesse võtma, kui nad hindavad üksikute ärisuhete ja juhutehingutega seotud rahapesu ja terrorismi rahastamise riski. Suunised riskitegurite kohta. 04.01.2018. Arvutivõrgus: https://www.fi.ee/sites/default/files/2018-08/pp_nr_10_Guidelines_on_Risk_Factors_ET_04-01-2018.pdf (14.03.2021).

41. European Data Protection Supervisor. Opinion 5/2020 on the European Commission's action plan for a comprahensive Union policy on preventing money laundering and terrorism financing. 23.07.2020. Arvutivõrgus: https://edps.europa.eu/sites/edp/files/publication/20-07-23_edps_aml_opinion_en.pdf. (17.02.2021)
42. European Data Protection Supervisor. Opinion on a Commission Proposal Amending Directive (EU) 2015/849 and Directive 2009/101/EC, Acess to beneficial ownership information and data protection implications. Arvutivõrgus: https://edps.europa.eu/sites/default/files/publication/17-02-02_opinion_aml_en.pdf (15.03.2021).
43. FATF. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations. Updated October 2020. Arvutivõrgus: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf (21.04.2021).
44. FATF. Jurisdictions under Increased Monitoring – February 2021. Arvutivõrgus: http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-february-2021.html (29.02.2021).
45. Financial Action Task Force (FATF) ''Guidance. Politically exposed persons (recommentadions 12 and 22)''. Arvutivõrgus: http://www.fatf-gafi.org/media/fatf/documents/recommendations/guidance-pep-rec12-22.pdf. (17.04.2021).
46. Finantsinspektsiooni 18.03.2020 juhatuse otsus nr 4.1-1/40. Ettekirjutus Swedbank AS-le nõudmises viia oma tegevus kooskõlla krediidiasutuste tegevust reguleerivate õigusaktidega.
47. Finantsinspektsiooni 19.02.2019 juhatuse otsus nr 4.1-1/8, ''Ettekirjutus Daske Bank A/S-le''.
48. Finantsinspektsiooni soovituslik juhend ''Krediidi-ja finantseerimisasutuste organisatsiooniline lahend ning ennetavad meetmed rahapesu ja terrorismi rahastamise tõkestamiseks''. Arvutivõrgus: https://www.fi.ee/sites/default/files/2018-11/FI_AML_Soovituslik_juhend.pdf (21.04.2021).
49. Freedman, B. Officially Blacklisted Extremist Terrorist (Support) Organizationz: a Comparison of Lists from six Countries and two International Organizations. Perspectives on Terrorism: May 2010 vol 4, No 2, pp. 46-52. Arvutivõrgus: https://www.jstor.org/stable/pdf/26298448.pdf (21.04.2021)

50. Inbank AS üldtingimused. Arvutivõrgus: https://www.inbank.ee/documents/ee/et/pdf/general_conditions_3.pdf (13.04.2021)
51. Rahandusministeeriumi juhend. Juhis tegeliku kasusaaja määratlemiseks. Rahandusministeerium. Arvutivõrgus: https://www.rahandusministeerium.ee/sites/default/files/tegelike_kasusaajate_andmete_esitamise_juhis_.pdf (21.02.2021).
52. Seletuskiri isikuandmete kaitse seaduse eelnõu juurde. Arvutivõrgus: Arvutivõrgus: https://www.aki.ee/sites/default/files/dokumendid/reform/iks_sk_21.03.18.pdf (20.03.2021).
53. Seletuskiri rahapesu ja terrorismi rahastamise tõkestamise seaduse eelnõu juurde. Arvutivõrgus: https://m.riigikogu.ee/tegevus/eelnoud/eelnou/fb03e20e-caf7-463d-9b60-ddf6021742b2/Rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20seadus (14.03.2021).
54. Swedbank AS. ''Kliendiandmete töötlemise põhimõtted''. Arvutivõrgus: https://www.swedbank.ee/static/pdf/private/home/important/gdpr/Principles_of_processing_Personal_data_EE_EST_01032021.pdf (20.03.2021).
55. Teave AS SEB panga arvelduskonto avamisest. Arvutivõrgus: https://www.seb.ee/igapaevapangandus/kontod-ja-arveldused/arvelduskonto (12.04.2021).
56. WP29. Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Direcitove 95/46/EC. 09.04.2014. Arvutivõrgus: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (29.03.2021).
57. WP29. Opinion 15/2011 on the definition on consent. Arvutivõrgus: https://www.pdpjournals.com/docs/88081.pdf (22.03.2021).
58. WP29. Opinion 03/2013 on purpose of limitation. Arvutivõrgus: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (15.03.2021).