Täiendavad selgitused Rahapesu Andmebüroo 25.04.2022 kinnitatud kahtlaste tehingute tunnuste juhendi tõlgendamiseks: terrorismi rahastamise riski ja kahtluse teated

Kellelt: Rahapesu Andmebüroo
Kellele: RahaPTSi järgi kohustatud isikud
Kuupäev: 06.01.2023

Kõigile RahaPTSi järgi kohustatud isikutele kehtib 25.04.2022 kinnitatud kahtlaste tehingute tunnuste juhend. Rahapesu Andmebüroo teate esitamise süsteem on juhendiga vastavuses kuupäevaks 11.01.2023. Samaks kuupäevaks viivad teadete monitooringu- ja esitamissüsteemid juhendiga vastavusse ka krediidiasutused.

Kahtlaste tehingute tunnuste juhendi eesmärk on tõhusam terrorismi rahastamise tõkestamine. Juhendis väljatoodud TFR-1 indikaatorid viitavad terrorismi rahastamise (TF) riskile ning TFR-2 indikaatorid terrorismi rahastamise kahtlusele. See tähendab, et **TFR-1** all on **riskiindikaatorid,** milles on ebaharilikkuse tunnused, ja **TFR-2** all **kahtlusindikaatorid**, mis võivad osutada potentsiaalsele terrorismi rahastamisele. Indikaatorid aitavad turuosalistel terrorismi rahastamisele viitavates märkides paremini orienteeruda ning kohaldada seetõttu ka riskile vastavaid hoolsusmeetmeid.

Juhendi TF-indikaatorid on ohumärgid, mis toovad välja potentsiaalselt terrorismi rahastamisele (TF) viitavad asjaolud. Need osutavad võimalikule mõistliku selgituse puudumisele, ebaharilikkusele, võivad tuua kaasa kahtluse. Riski- ja kahtluspõhised indikaatorid lähtuvad varasematest kaasustest, jälitusteabest, ohuhinnangutest, analüüsidest, finantsteabest ning terrorismi rahastamise trendidest ja tüpoloogiatest (sh FATFi, Egmont Groupi, EUROPOLi avalikud raportid).

Indikaatorid on seotud kontekstipõhiste asjaoludega, mis aitavad tuvastada tehingu või toimingu juures ebaharilikkust või kahtlust, et tegu võib olla terrorismi rahastamisega. Kooskõlas hoolsusmeetmete kohaldamisega, taustateadmistega kliendi ja tehingu/toimingu konteksti kohta toetavad indikaatorid kohustatud isiku hinnangut, sh kahtlust või ebaharilikkust, kas tehingu või toimingu eesmärk võib olla terrorismi rahastamine. Indikaatorite näol ei ole tegu ammendava nimekirjaga: indikaatorid ei kata iga võimalikku tehingut või toimingut, mis võib olla seotud terrorismi rahastamisega.

TF-riskiindikaatorite põhjal tuleb esitada teateid (TFR-1) lähtuvalt ebaharilikkuse printsiibist. See tähendab, et tehingu või toimingu kokkulangemine TF-riskiindikaatoriga vajab kohustatud isiku poolt hoolsusmeetmete kohaldamist ja analüüsi. Kui tehing või toiming langeb kokku TF-riskiindikaatoriga, kuid kohustatud isik hindab põhjalikuma analüüsi järel, et puudub ebaharilikkus, ei ole teate esitamine vajalik. Analüüsi käigus võtab kohustatud isik lisaks juhendis väljatoodud terrorismi rahastamise indikaatoritele arvesse hoolsusmeetmete kohaldamisel kogutud infot, sh taustainfot, kliendiprofiili ja tehingu/toimingu laiemat konteksti. Teade tuleb esitada aga tingimata, kui esineb kahtlus (TFR-2) või mistahes ebaharilikkus (TFR-1).

Rahapesu Andmebüroo poole on pöördutud enim seonduvalt küsimustega riskiindikaatorite (TFR-1) 3, 7, 14, 15, 18, 20 ja 31 kohta. Seetõttu soovitab Rahapesu Andmebüroo kooskõlas Kaitsepolitseiametiga toetuda järgmistele põhimõtetele. Tehingu või toimingu hindamisel TF-riskiindikaatori perspektiivist tuleks võtta aluseks lähtepunkt, kas tehing või toiming on ebaharilik, kas see on kliendi profiili ning väidetava tehingu eesmärgiga kooskõlas.

Kui tehingu või toimingu juures ei ole ebaharilikkust (TFR-1) ega kahtlust (TFR-2) või muid juhendis toodud indikaatoreid, ei ole teate esitamine Rahapesu Andmebüroole vajalik.

Järgnevalt toob Rahapesu Andmebüroo välja mõningad selgitused, kuidas TF-riskiindikaatoreid (TFR-1) paremini tõlgendada, et esitada Rahapesu Andmebüroole teade.

1. TF-riskiindikaator nr 3, mille eeldus on seos riskiriigiga. (**Esmakordne tehing füüsilise/juriidilise isikuga või muu ühendusega riskiriigis.**) [1] Teade tuleb esitada iga esmakordse tehingu korral füüsilise/juriidilise isikuga või muu ühendusega riskiriigis, mis on kliendi profiili või muid asjaolusid arvestades ebaharilik. Näiteks teeb riskiriigi seosega isik tehingu (sh sularahasiire), mille puhul ei ole tehingu eesmärk selge või ei lange see kokku tema profiiliga vm.

2. TF-riskiindikaator nr 7, mille eeldus on seos riskiriigiga. (**Sagedane sularaha sissemakse arveldusarvele.**) Väljend „sagedane" on jäetud teadlikult defineerimata: selle tõlgendamisel tuleks lähtuda ebaharilikkuse põhimõttest. Kui isiku tehingud või toimimisviis on kliendi profiili ja/või Eesti konteksti arvestades ebaharilik, tuleb esitada teade.

Näide. Riskiriigi seosega väikeettevõtja kasutab kauplemisel sularaha ning teeb pidevalt sularaha sissemakseid. Käitumismuster on teiste klientidega võrreldes ebaharilik, mistõttu tuleb sellest teada anda.

3. TF-riskiindikaator nr 14, mille eeldus on seos riskiriigiga. (**Kontoga seotud pangakaardi (ka lisakaart) samaaegne või ajaliselt lähestikku kasutamine eri riikides või piirkondades, kui vahemaa füüsiline läbimine ei ole selle ajavahemiku jooksul realistlik.**) Teade tuleb esitada, kui ilmneb ebaharilikkus. Juriidilise isiku puhul tuleb esitada teade **pangakaardi valdaja** ehk konkreetse füüsilise isiku kohta.

4. TF-riskiindikaator nr 15, mille eeldus on seos riskiriigiga. (**Kliendi pangakaardi/konto on seotud teise makseteenuse pakkuja teenuse külge (näiteks sidumine rahvusvahelise finantsteenuse platvormiga.**) Teade tuleb esitada, kui ilmneb ebaharilikkus. Indikaatori eesmärk on tuvastada tehinguid, mida tehakse makseteenuse pakkuja kaudu, et varjata tehingute jälgi ja sisu (nt plahvatusohtlike ainete tellimine jm).

Kuivõrd krediidiasutused ei näe sidumise fakti, vaid ainult tehingut, siis esitab krediidiasutus teateid just rahvusvahelise finantsteenuse platvormiga tehtud **tehingute** kohta, mida hindab kliendi profiili või muid asjaolusid arvestades ebaharilikuks.

5. TF-riskiindikaator nr 18, mille eeldus on seos riskiriigiga. (**Kliendi sidevahendi IP-aadress viitab riskiriigile (maksete tegemisel, kontole logimisel) või ebaharilikule VPN-ühenduse kasutamisele, muule asukoha või identiteedi varjamisele või muutub ebaharilikult tihti.**)[2]

Teade tuleb esitada, kui kliendi profiili arvestades nähtub ebaharilikkus. Ebaharilik VPNi kasutamine on näiteks olukord, kus isiku osutatud asukoht muutub selliselt, et vahemaa füüsiline läbimine ei ole ajavahemiku jooksul realistlik. (Teadet ei ole tarvis esitada, kui nähtub IP-aadressi muutmine sama riigi sees.) Samuti võib selleks kvalifitseeruda olukord, kus nähtuv asukoht on kliendi profiili arvestades ebaharilik, sh riskiriigis viibimise varjamise eesmärgil VPNi kasutamine. Riskiriigile viitav IP-aadress ning identiteedi varjamisele osutav käitumine võib viidata terrorismi rahastamisele ka isiku puhul, kelle profiili arvestades ei ole riskiriigis viibimine ebatavaline.

6. TF-riskiindikaator nr 20, mille eeldus on seos riskiriigiga. (**Kliendisuhte loomine ja/või esmakordne tehing viitab seotusele riskiriigiga (näiteks sünnikoht, aadress, telefoninumber, e-posti aadress, IP-aadress).**)

Teade tuleb esitada, kui riskiriigi seosega isiku puhul on kliendisuhte loomise ja/või esmakordse tehingu juures mistahes ebaharilikkus. Näiteks viitavad riskiriigi seosega isiku logi- ja/või sideandmed teisele riskiriigile, esimese kandena nt krüptoraha soetamisel toimuvad laekumised riskiriigiga seotud isiku kontolt (FIAT makse krüptovääringu soetamiseks, krüptovääringu FIATisse konverteerimine), andmete esitamisel sisuline ebatäpsus, puudulik info või üldsõnalisus, kliendi profiilile mittevastav tehing; kliendi profiili või käitumise juures esineb muud ebaharilikkust (sh avalike allikate põhjal). Ebaharilikkusele osutav käitumine võib viidata terrorismi rahastamisele ka isiku puhul, kelle profiili arvestades ei ole riskiriigis viibimine ebatavaline.

Näide. Riskiriigiga seotud isik külastab mitu korda aastas riskiriiki ning tugevdatud hoolsusmeetmete kohaldamise käigus ei ole klient andnud ammendavaid selgitusi.

[1] Sarnane indikaator oli ka eelmises ehk 2019. aasta juhendis – „Esmakordne tehing füüsilise/juriidilise isikuga riskiriigis".
[2] Sarnane indikaator oli ka eelmises ehk 2019. aasta juhendis – „Kliendi arvuti IP aadress viitab riskiriigile (maksete tegemisel, kontole logimisel)".

7. TF-riskiindikaator nr 31, mille eeldus on seos riskiriigiga. (**Sularaha sissemaksetest pärinevate vahendite saatmine mittetulundusühingule, sihtasutusele või muule sarnasel eesmärgil loodud ühendusele/organisatsioonile, mis tegutseb riskiriigis või mis osutab abi või teenuseid riskiriigiga seotud isikutele**.)[3]

Krediidiasutus ei pruugi olla kursis asjaoluga, et tehingu vastaspool on riskiriigis tegutsev mittetulundusühing või sarnasel eesmärgil loodud organisatsioon. Seetõttu esitab krediidiasutus teate, kui **mittetulundusühing, sihtasutus või muu sarnasel eesmärgil loodud ühendus/organisatsioon, mis tegutseb riskiriigis või mis osutab abi või teenuseid riskiriigiga seotud isikutele**, on krediidiasutuse klient ning talle saadetakse sularaha sissemaksetest pärinevaid vahendeid, mis võivad viidata terrorismi rahastamisele. (NB. Spetsiifiliselt MTÜde sektori tegevusvaldkonda puudutavad ka riskiindikaatorid nr 28, 29, 30 ja 32.)

[3] Kaks sarnast indikaatorit olid ka eelmises ehk 2019. aasta juhendis – „Isik teostab ülekande mittetulundusühingu kontole (NGO, NPO), mis tegutseb riskiriigis või mille tegevusalaks on riskiriikidele abi osutamine“ ning „Tehing riskiriigis tegutseva mittetulundusühinguga“.