

RAHAPESU JA TERRORISMI RAHASTAMISE TÕKESTAMISE POLIITIKA

POLIITIKA EESMÄRK JA ALUSED

Poliitika õiguslikuks aluseks on Eesti Vabariigi ja Euroopa Liidu õigusaktid, rahvusvahelised lepingud ja konventsioonid, rahvusvaheliste organisatsioonide juhised ja järelevalveorganite juhendid.

Poliitika eesmärgiks on kehtestada aluspõhimõtted ja üldised tegevussuunised tagamaks efektiivse ning proportsionaalset rahapesu ja terrorismi rahastamise tõkestamise meetmete rakendamist CoinEx Group OÜ -s, edaspidi Äriühingus.

Äriühing asutati 12.12.2002, äriühingu koduleht asub aadressil: <https://coinex.cash/> Rahapesu ja terrorismi rahastamise tõkestamise alast tegevust korraldab ja selle eest vastutab Äriühingu juhatuse liige või juhatuse liikme poolt määratud Rahapesu andmebüroo kontaktisik.

Äriühingu riskid ja nende maandamise meetmed on kindlaksmääratud Riskihinnanguga, samuti määratakse Riskihinnangus kindlaks Äriühingu riskiisu.

Äriühing lähtub rahapesu ja terrorismi rahastamise tõkestamisel tunne-oma-klienti põhimõttest. "Tunne oma klienti" põhimõtte efektiivse toimimise üheks peamiseks eelduseks on võimalikult täpsete ja põhjalikke andmete kogumine kliendisuhete loomisel. See võimaldab kliendi poolt esitatud andmete alusel positsioneerida tema esialgset riskiastet ning hinnata kliendi maksekäitumise vastavust, tema poolt esitatud andmetele.

Riskipõhine lähenemine, andmete kogumine ja uuendamine, tehingute monitoorimine ja vara päritolu tõendavate dokumentide analüüsimine on meetmed, mille kohaldamise tulemusena peab Äriühingul tekkima kliendist tervikpilt ja sisemine veendumus kliendi tegevuse seaduspärasuse osas.

Äriühing rakendab "tunne oma klienti" põhimõtet kogu kliendisuhete vältel. Äriühing hindab ja analüüsib regulaarselt rahapesu ja terrorismi rahastamise alaseid riske ning on kehtestanud üksikasjalikud rahapesu ja terrorismi rahastamise tõkestamise alased tegevusjuhised Äriühingu töötajatele.

Konkreetsed juhised rahapesu ja terrorismi rahastamise tõkestamiseks on kindlaksmääratud juhendis " Protseduurireeglid rahapesu ja terrorismi rahastamise tõkestamiseks ".

Äriühingu töötajad on kohustatud kõrvalekaldumatult järgima õigusaktides ja sisereeglites sätestatud juhiseid rahapesu ja terrorismi rahastamise tõkestamiseks.

ÄRIÜHINGU TEGEVUSVALDKONNAD

Äriühing tegutseb Rahapesu Andmebüroo poolt väljastatud tegevuslubade alusel ning kuulub RAB-i järelevalve alla, Äriühing osutab järgmiseid teenuseid:

1. valuutavahetus, tegevusloa number VVT000337

2. pandimaja teenused (laen kulla tagatisel), tegevusloa number FIP000170
3. virtuaalvääringu rahakotiteenus, tegevusloa number FVT000080
4. virtuaalvääringu vahetus läbi BATM-i ja Äriühingu esinduses, tegevusloa number FVT000080
5. finantseerimisasutusena tegutsemine, tegevusloa number FFA000144.

Kõikki teenuseid osutatakse vaid viibides isikuga füüsiliselt samas kohas st Äriühingu esindustes ning kõik isikud tuvastatakse olenemata tehingusumma suuruselt (välja arvatud valuutavahetus sularahas kuni 1000 eurot). Äriühing ei paku oma klientidele virtuaalvääringu makse teenuseid. Äriühing kontorid asuvad Tallinnas aadressidel Tartu mnt. 51-3A ja Laikmaa 5 ning Tartus aadressil Küüni 7.

BATM-i kasutades on võimalik tehinguid teha ainult sularahas, BATM-i CRM programm võimaldab ühel kliendil teha tehinguid kuni 1000 eurose limiidi piires.

RISKIJUHTIMISE SÜSTEEM

Kõik Äriühingu töötajad peavad tagama oma vastutusalas olevate tegevuste, toodete ja protsessidega seotud riskide tuvastamise, hindamise ning piisavate kontrollimehhanismide rakendamise tuvastamiseks puuduseid ja vigu töötajate tegevuses, tööjuhendites, protseduurides või protsessides. Tagamaks antud põhimõtte täitmist, on Äriühing jaotanud riskijuhtimise ülesanded vastavalt rahvusvahelisele kolme kaitseliini meetodile.

I kaitseliin

Esimese kaitseliini moodustavad CRM programm ja klienditeenindajad, kelle ülesandeks on hoolsusmeetmete kohaldamine ärisuhte loomisel sh kliendi isikusamasuse tuvastamine ja tunne oma klienti põhimõtte rakendamine sellisel, et saadud info alusel oleks võimalik määrata kindlaks kliendi riskiprofiil ja riskiaste ning hilisem ärisuhte seire. Programmi tööd kontrollivad RAB kontaktisik ja sisekontroll.

II kaitseliin

Teise kaitseliini moodustavad vastutav juhatuse liige ja RAB kontaktisik.

Vastutav juhatuse liige tagab Äriühingu protsesside/toodetega/teenustega seotud riskide tuvastamise, hindamise ja juhtimise sh korraldab riskitegurite kaardistamise ja analüüsi hindamiseks kehtivate rahapesu ja terrorismi rahastamise tõkestamise alaste meetmete sobivust ning vastutab õigusaktidele ja järelevalve juhistele vastava sisereeglistiku olemasolu eest.

RAB kontaktisik omab kord poolaastas aruandluskohustust juhatuse ees. RAB kontaktisiku ülesandeks on teabe kogumine ebaharilike, rahapesu kahtlusega ja/või terrorismi rahastamisele viitava iseloomuga tehingute kohta, vastava teabe analüüsimine ja vajadusel edastamine Rahapesu andmebüroole ning viimase ettekirjutuste täitmine ning töötajate koolitamine. RAB kontaktisik vastutab ka rahvusvahelisest sanktsiooniseadusest tulenevate kohustuste täitmise eest.

III kaitseliin

Kolmanda kaitseliini moodustab Äriühingu audiitorettevõtja, kes teostab raamatupidamise aastaaruande audiitorkontrolli ja omavahendite kohta kehtestatud nõuete täitmise kontrolli

ning esitab majandusaasta aruande esitamise tähtjaks sellekohase arvamuse nii Äriühingule, kui ka Rahapesu Andmebüroole ja siseaudiitor, kes kontrollib regulaarselt juhatuse, RAB kontaktisiku, klienditeenindajate ja IT lahenduste vastavust õigusaktides, järelevalve juhistes ja CoinEx Group OÜ sisereeglites sätestatud nõuetele. Siseaudit teeb juhatusele ettepanekuid kontrollimise käigus ilmnunud puuduste kõrvaldamiseks ning siseprotseduuride muutmiseks ja täiendamiseks.

RISKIDE HINDAMINE

Läbi riskide pideva hindamise püüab Äriühing minimiseerida võimalust, et tema teenuseid võidakse kasutada rahapesuks või terrorismi rahastamiseks. Iga-aastased ning *ad hoc* riskihinnangud dokumenteeritakse ning tehakse töötajatele ja vajadusel järelevalve organitele kättesaadavaks.

Riskide tuvastamiseks, hindamiseks ja analüüsimiseks võetavad meetmed peavad vastama äritegevuse laadile ja keerukusele. Riskide hindamise järgselt tuleb ette näha meetmeid, millega riskid tulemuslikult maandatakse. Riskide hindamise raames tuvastatakse, millised on peamised riskitegurid, kui suur on nende realiseerumise tõenäosus ning millises ulatuses peab riskide maandamiseks kohaldama hoolsusmeetmeid. Peamiseks rahapesu ja terrorismi rahastamise alaste riskide maandamise meetmeks on hoolsusmeetmete proportsionaalne ja riskipõhine kohaldamine. Riskide efektiivseks juhtimiseks ja maandamiseks on äärmiselt oluline töötajatele operatiivsete juhiste andmine.

Riskide hindamiseks kogutakse kliendi kohta andmeid, mis võimaldavad määratleda kliendi profiili ja saada aru kliendiga ning tema tehingutega seotud riskidest. Riskide määramisel arvestatakse erinevaid riskikategooriaid kogumis ning määratakse kliendile riskiaste. Kliendi suhtes kohaldatavate hoolsusmeetmete ulatus sõltub kliendi riskiastmest.

Riskiastme määramine toimub kindlaksmääratud kriteeriumite põhjal, mille alusel selgitatakse välja väikese, tavapärase ja suure riskitasemega kliendid ning otsustatakse, milliste klientide või teenuste puhul piisab lihtsustatud või tavapäraste hoolsusmeetmete kohaldamisest ja milliste puhul on nõutav kohaldada tugevdatud hoolsusmeetmeid.

Riskiastme määramine ja muutmine eeldab pidevat ärisuhte seiret, sealhulgas ärisuhte vältel teostatud tehingute analüüsimist, tagamaks, et teostatud tehingud on kooskõlas Äriühingu teadmistega Kliendist, tema tegevusest ja selle vastavusest kliendile määratud riskiastme kriteeriumitele.

HOOLSUSMEETMED

Sõltuvalt kliendi riskiprofiilist kohaldab Äriühing kas tavapäraseid või tugevdatud hoolsusmeetmeid. Hoolsusmeetmete valiku ja kohaldamise ulatuse alused on Äriühing kindlaks määranud Riskihinnangu dokumendis. Detailsed juhised Äriühingu töötajatele hoolsusmeetmete kohaldamiseks on sätestatud Protseduurireeglid rahapesu ja terrorismi rahastamise tõkestamiseks juhendis.

Äriühing lähtub hoolsusmeetmete kohaldamisel riskipõhisest lähenemisest, kohaldab "tunne oma klienti" põhimõtet ning teostab pidevat klientide ja tehingute seiret.

Äriühing tagab kõikide töötajate rahapesu ja terrorismi rahastamise tõkestamise alase koolituse läbimise enne tööle asumist ning hilisema koolitamise vastavalt vajadusele, kuid mitte harvemini kui üks kord aastas.

KLIENDIPROFIILI VÄLISTUSED

Äriühing on määratlenud rea kriteeriume ja tunnuseid, mille esinemise korral kliendiprofiilis Äriühing isikuga ärisuhtesse ei astu:

- 1) isikutega, kelle osas ei suudeta täita hoolsusmeetmeid;
- 2) isikutega, kelle osas on varasemalt teada või tekib hoolsusmeetmete kohaldamise käigus rahapesu ja/või terrorismi rahastamise kahtlus;
- 3) anonüümsete ja/või fiktiivsete isikutega ning variisikutega;
- 4) varipankadega ja selliste krediidasutuste või finantseerimisasutustega, kes teadaolevalt lubavad varipankadel oma kontosid kasutada (korrespondentsuhteid ei looda);
- 5) sanktsiooni subjektidega - isikutega, kes on kantud UN, OFAC ja EU sanktsiooni nimekirjadesse;
- 6) füüsiliste või juriidiliste isikutega, kes on pärit FATF riskiriikidest (kus ei rakendata piisavalt meetmeid rahapesu- ja terrorismi rahastamise tõkestamiseks);
- 7) tumbler/mikser teenuste pakkujatega;
- 8) isikutega, kelle kapitalist rohkem kui 10 protsenti moodustavad esitajaaktsiad või muud esitajaväärtpaberid;

POLIITIKA AJAKOHASTAMINE

Äriühingu juhatus vaatab Rahapesu ja terrorismi rahastamise tõkestamise poliitika vastavuse õigusaktid, Äriühingu majandustegevust ja riskijuhtimise mudelit üle kord aastas ning vajadusel ajakohastab Poliitikat.