UAB CHRONOS GLOBAL

Konstitucijos pr. 26,
LT-08131 Vilnius, Lietuva
info@columis.com

MŪSŲ ĮSIPAREIGOJIMAS KOVOTI SU PINIGŲ PLOVIMU IR TERORIZMO FINANSAVIMU

UAB „Chronos Global“ yra įsipareigojusi užtikrinti saugią ir reikalavimus atitinkančią aplinką visiems savo klientams. Būdami kriptoturto paslaugų teikėju Lietuvoje, veikiame pagal griežtus reguliavimo reikalavimus, siekdami užkirsti kelią pinigų plovimui, teroristų finansavimui, sukčiavimui ir kitai neteisėtai veiklai.

Manome, kad finansų ir kriptoturto sektoriuose būtinas skaidrumas ir pasitikėjimas. Mūsų patikima kovos su pinigų plovimu sistema užtikrina, kad mūsų platforma būtų saugi, patikima ir atitiktų Lietuvos Respublikos įstatymus, Europos Sąjungos direktyvas ir geriausią tarptautinę praktiką.

Siekdami apsaugoti savo platformą nuo finansinių nusikaltimų, taikome rizika pagrįstą požiūrį ir pažangiausias kovos su pinigų plovimu priemones. Tai apima griežtą klientų patikrą, operacijų stebėseną ir atitiktį „Travel Rule“ reikalavimams, kad būtų užkirstas kelias tokiai neteisėtai veiklai kaip pinigų plovimas, teroristų finansavimas, sukčiavimas ir sankcijų vengimas.

Kaip saugome savo platformą ir klientus

1. Deramas klientų pažinimas (angl. Know Your Customer - KYC) ir klientų tikrinimas (angl. Client Due Diligence - CDD)

Prieš pradėdamas naudotis mūsų paslaugomis, kiekvienas klientas pereina griežtą tapatybės patikrinimo procesą. Tai yra:

- Tapatybės patikrinimas naudojant patikimus ir nepriklausomus duomenų šaltinius.
- Asmeninės ir verslo informacijos rinkimas privačių ir verslo klientų atveju.
- Patikra sankcijų sąrašuose ir politiškai pažeidžiamų asmenų (PEP) duomenų bazėse.
- Nuolatinė klientų stebėsena siekiant užtikrinti nenutrūkstamą atitiktį.

Taikome deramo patikrinimo procesus, atsižvelgdami į kiekvieno kliento rizikos lygį:

- Standartinis deramas kliento patikrinimas (angl. Client Due Diligence - CDD) – taikomas visiems klientams, vykdantiems standartines operacijas.
- Sustiprintas deramas kliento patikrinimas (angl. Enhanced Due Diligence - EDD) – taikomas didelės rizikos klientams, įskaitant klientus iš didelės rizikos jurisdikcijų arba klientus, vykdančius sudėtingas operacijas, keliančius aukštesnę pinigų plovimo ir terorizmo finansavimo riziką.

Pasikeitus kliento rizikos profiliui, galime prašyti papildomos informacijos arba imtis papildomų veiksmų galimai rizikai sumažinti.

2. Atitiktis „Travel Rule“ taisyklei

Laikomės „Travel Rule“ taisyklės, nustatytos Reglamente (ES) 2023/1113, užtikrinančios kriptoturto sandorių skaidrumą. Tai reiškia, kad:

Klientui siunčiant arba gaunant kriptoturtą, mes renkame, tikriname ir dalijamės pagrindine operacijos informacija su gaunančiuoju arba siunčiančiuoju subjektu.

Jei sandorio šalies kriptoturto paslaugų teikėjas nesilaiko „Travel Rule“ taisyklės, mes, siekdami sumažinti atitikties riziką, galime blokuoti arba atmesti operaciją.

Šiomis priemonėmis užtikrinama, kad visos operacijos kriptoturtu atitiktų finansinio skaidrumo standartus ir būtų užkirstas kelias neteisėtiems lėšų pervedimams.

3. Operacijų stebėsena ir pranešimai apie įtartiną veiklą

Siekdami nustatyti neįprastas ar įtartinas operacijas, naudojame pažangias realaus laiko stebėjimo priemones. Naudojame tiek automatinius, tiek rankinius metodus, siekdami aptikti, bet neapsiribojant žemiau išvardintais kriterijais:

- Didelės vertės operacijas, įskaitant operacijas, viršijančias 15 000 eurų (arba lygiavertę sumą kriptoturtu):
- Neįprastus operacijų modelius, kai nukrypstama nuo kliento įprasto elgesio.
- Pervedimus į didelės rizikos jurisdikcijas arba iš jų.
- Operacijas, susijusias su žinomomis didelės rizikos kriptovaliutų piniginėmis arba su tamsiuoju internetu (angl. *darknet*) susijusia veikla.

Jei nustatoma įtartina veikla, imamės neatidėliotinų veiksmų, įskaitant, bet neapsiribojant žemiau išvardintais:

- Operacijos užblokavimas siekiant atlikti tolesnį tyrimą.
- Pranešimo apie įtartiną veiklą pateikimas Finansinių nusikaltimų tyrimo tarnybai (FNTT) Lietuvoje.
- Prašymas, kad klientai pateiktų papildomą informaciją, patvirtinimus ar dokumentus.
- Sąskaitų, neatitinkančių atitikties reikalavimų, uždarymas.

4. Sankcijų laikymasis ir patikra

Griežtai laikomės tarptautinių sankcijų ir imamės aktyvių priemonių, kad mūsų platforma nebūtų naudojama neteisėtai veiklai. Mūsų sistema automatiškai atlieka šias, bet neapsiribojant žemiau pateiktomis, patikras:

- Visų klientų ir sandorių – Europos Sąjungos (ES), Jungtinių Tautų (JT), Jungtinių Amerikos Valstijų (OFAC), Jungtinės Karalystės (HMT) ir Lietuvos Respublikos institucijų sankcijų sąrašuose.

- Kriptovaliutų sandorių, kuriuose dalyvauja su finansiniais nusikaltimais susiję įspėjamuoju ženklu pažymėti arba į juodąjį sąrašą įtraukti adresai.
- Dalykinių santykių, susijusių su subjektais ar asmenimis iš jurisdikcijų, kurioms taikomos sankcijos.

Jei nustatomas asmuo, subjektas ar operacija, kuriai taikomos sankcijos, mes:

- Tuojau pat įšaldome su juo susijusią sąskaitą arba lėšas.
- Pranešame apie atvejį atitinkamoms institucijoms.
- Visapusiškai bendradarbiaujame su teisėsaugos institucijomis, kad būtų užkirstas kelias pažeidimams.

5. Rizika pagrįstas metodas ir vidaus kontrolė

Siekdami užtikrinti veiksmingą atitiktį, esame įdiegę trijų gynybos linijų modelį:

1. Pirmoji gynybos linija – mūsų tiesiogiai su klientais dirbantys darbuotojai užtikrina, kad užmezgant dalykinius santykius su klientais, atliekant operacijas ir vykdant nuolatinę stebėseną būtų laikomasi kovos su pinigų plovimu ir teroristų finansavimo procedūrų.
2. Antroji gynybos linija – mūsų rizikos ir atitikties užtikrinimo skyrių darbuotojai, įskaitant pinigų plovimo prevencijos pareigūną, prižiūri pinigų plovimo ir teroristų finansavimo prevencijos kontrolės priemones, tiria įtartiną veiklą ir užtikrina atitiktį teisės aktų reikalavimams.
3. Trečioji gynybos linija – mūsų nepriklausomas vidaus auditas peržiūri pinigų plovimo ir teroristų finansavimo prevencijos procedūras, įvertina riziką ir užtikrina mūsų atitikties sistemos veiksmingumą.

Mūsų pinigų plovimo ir teroristų finansavimo prevencijos politika peržiūrima bent kartą per metus, atsižvelgiant į reguliavimo pokyčius, naujas grėsmes ir geriausią praktiką.

6. Darbuotojų mokymas ir informuotumas

Manome, kad žinios yra veiksmingos kovos su pinigų plovimu ir teroristų finansavimu pagrindas. Todėl investuojame į reguliarius mokymus kovos su pinigų plovimu, teroristų finansavimu ir atitikties temomis visiems darbuotojams, įskaitant:

- Privalomą kasmetinį visų darbuotojų mokymą apie finansinių nusikaltimų riziką.
- Specializuotus mokymus atitikties užtikrinimo darbuotojams ir vyresniesiems vadovams.
- Realių atvejų scenarijų pratybas, skirtas pagerinti įtartinos veiklos nustatymą ir reagavimą į ją.
- Nuolat atnaujinamą informaciją apie naujausius kovos su pinigų plovimu ir teroristų finansavimu teisės aktus ir pokyčius sektoriuje.

7. Saugus duomenų rinkimas ir saugojimas

Siekdami laikytis teisės aktų reikalavimų, saugiai laikome klientų tapatybės nustatymo ir operacijų duomenis:

- klientų ir operacijų įrašus – 8 metus.
- su atitiktimi susijusius komunikacijos įrašus – 5 metus.

Užtikriname visišką BDAR ir duomenų apsaugos įstatymų laikymąsi, todėl jūsų asmeninė ir finansinė informacija visada saugoma ir konfidenciali.

Finansinių nusikaltimų netoleravimo politika

UAB „Chronos Global“ griežtai pasisako prieš pinigų plovimą, terorizmo finansavimą, sukčiavimą ir kitą neteisėtą veiklą. Mes nedirbame su:

- Klientais iš šalių, su kuriomis uždrausta dirbti arba kurioms taikomos sankcijos.
- Neskaidrios nuosavybės struktūros įmonėmis.
- Klientais, kurių veikla kelia didelę finansinių nusikaltimų riziką.
- Neužsiimame jokia veikla, kuri neatitinka bendrovei priimtinos rizikos lygio.

Klientui nesilaikant mūsų atitikties standartų, pasiliekame teisę atsisakyti užmegzti dalykinius santykius arba juos nutraukti.

Saugios ir skaidrios kriptoturto ekosistemos kūrimas

Esame įsipareigoję suteikti saugią ir reikalavimus atitinkančią platformą, kuri apsaugotų mūsų klientus, bet ir palaikytų kriptoturto srities inovacijas.

Jei turite klausimų dėl mūsų pinigų plovimo ir teroristų finansavimo prevencijos politikos ar atitikties priemonių, kreipkitės į mus adresu info@columis.com.