AML/KYC саясаты

Осы AML/KYC саясаты («Саясат») Kazakhstan тіркелген F-Tech компаниясының («Компания», «біз», «бізді», «біздің») https://kashbi.io веб-сайтын, KashBi қолданбасын, Telegram-ботты, Telegram Mini App-ты, web-нұсқаны, API-ді, крипто-фиат әмиянды, P2P-платформаны және Компанияның өзге де байланысты сервистерін, бірлесіп «Платформа» деп аталатын сервистерді пайдалану кезінде ақшаны жылыстатудың, терроризмді қаржыландырудың, санкцияларды айналып өтудің, алаяқтықтың және өзге де заңсыз немесе тыйым салынған қызметтің алдын алу тәсілін сипаттайды.

Осы Саясат Пайдалану шарттарының бөлігі болып табылады және Құпиялылық саясатымен, P2P-мәмілелер қағидаларымен, комиссиялар қағидаларымен, тәуекелдер туралы ескертулермен және Компанияның өзге де құжаттарымен бірге қолданылады.

Платформаны пайдалану, аккаунт жасау, балансты толықтыру, цифрлық активтерді шығару, P2P-мәміле жасау немесе қабылдау, тексеруден өту немесе Платформамен өзге түрде өзара әрекеттесу арқылы пайдаланушы осы Саясатпен танысқанын және оның ережелерін сақтауға келісетінін растайды.

Егер пайдаланушы осы Саясатпен келіспесе, ол Платформаны пайдалануды тоқтатуы тиіс.

1. Мақсаты және қолданылу аясы

1.1. Саясаттың мақсаты

Осы Саясаттың мақсаты — келесіге бағытталған негізгі қағидаттарды, қағидаларды және шараларды белгілеу:

- Платформаны ақшаны жылыстату үшін пайдаланудың алдын алу;
- терроризмді қаржыландырудың алдын алу;
- санкцияларды айналып өтудің алдын алу;
- алаяқтықтың, скамның, фишингтің және өзге де құқыққа қарсы қызметтің алдын алу;
- жоғары тәуекелді пайдаланушыларды, операцияларды, мекенжайларды және юрисдикцияларды анықтау және бағалау;
- цифрлық активтермен операцияларды және P2P-мәмілелерді мониторингтеу;
- қолданылатын заңнама талаптарын, серіктестердің, AML/KYC сервистерін жеткізушілердің, банктердің, төлем провайдерлерінің және құзыретті органдардың талаптарын орындау;
- пайдаланушыларды, Компанияны, Платформаны және Компанияның іскерлік беделін қорғау.

1.2. Қолданылу аясы

Осы Саясат Платформаның барлық пайдаланушыларына, соның ішінде келесі пайдаланушыларға қолданылады:

- крипто-фиат әмиян;
- P2P-платформа;
- Telegram Mini App;
- Telegram-бот;
- web-нұсқа;
- цифрлық активтерді толықтыру және шығару функциялары;
- ішкі аударымдар;
- егер мұндай функциялар қолжетімді болса, P2P-тен тыс фиат операциялары;
- қолдау қызметі және даулар.

1.3. Тәуекелге негізделген тәсіл

Компания тәуекелге негізделген тәсілді қолданады. Бұл KYC, AML-тексерулер, лимиттер, құжаттарды сұрату, күшейтілген тексеру, мониторинг, шектеулер және өзге де шаралар пайдаланушының, операцияның, юрисдикцияның, төлем әдісінің, цифрлық активтің, блокчейн-мекенжайдың, пайдаланушы мінез-құлқының және өзге факторлардың тәуекел деңгейіне пропорционалды түрде қолданылатынын білдіреді.

Платформа privacy-first ретінде позицияланады: Компания дербес деректерді жинауды барынша азайтуға және қажетсіз сәйкестендіру құжаттарын сұратпауға ұмтылады. Сонымен бірге privacy-first толық анонимділікті білдірмейді және егер бұл заңмен, Платформа қағидаларымен, серіктестер талаптарымен немесе осы Саясатпен талап етілсе немесе рұқсат етілсе, деректерді өңдеуді, пайдаланушыны тексеруді, транзакцияларды тексеруді, операцияларды шектеуді немесе ақпаратты құзыретті органдарға беруді жоққа шығармайды.

2. Терминдер мен анықтамалар

2.1. AML

AML — заңсыз жолмен алынған кірістерді жылыстатуға қарсы іс-қимыл шаралары, оның ішінде қаражаттың заңсыз шығу тегіне байланысты операцияларды анықтау, алдын алу, тергеу және шектеу.

2.2. KYC

KYC — «өз клиентіңді біл» рәсімі, ол тәуекелді, лимиттерді, операцияны, қолданылатын заңнаманы немесе серіктестердің талаптарын ескере отырып мұндай рәсім қажет болған жағдайда пайдаланушыны сәйкестендіруді, тексеруді және бағалауды қамтиды.

2.3. CDD

CDD — клиентті тиісінше тексеру, ол пайдаланушы, оның белсенділігі, қаражат көзі, операциялардың мақсаттары және тәуекел профилі туралы ақпаратты жинау мен талдауды қамтиды.

2.4. EDD

EDD — жоғары тәуекелді пайдаланушыларға, операцияларға немесе жағдайларға қолданылатын күшейтілген тексеру. EDD қосымша құжаттарды сұратуды, қаражат көзін растауды, транзакцияларды кеңейтілген талдауды, ашық дереккөздерді тексеруді, санкциялық және PEP-тексерулерді, сондай-ақ Компанияның жауапты тұлғалары деңгейінде одан әрі қызмет көрсетуді келісуді қамтуы мүмкін.

2.5. KYT

KYT — «өз транзакцияңды біл» рәсімі, ол операцияларды, блокчейн-мекенжайларды, қаражат көздерін, пайдаланушы мінез-құлқын, байланысты әмияндарды, P2P-паттерндерді және нақты операцияға қатысты өзге деректерді талдауды қамтиды.

2.6. PEP

PEP — саяси маңызы бар тұлға, сондай-ақ оның отбасы мүшелері және осындай тұлғамен тығыз байланысты адамдар, егер мұндай тұлғалар сыбайлас жемқорлық, санкциялық, беделдік немесе өзге тәуекелдер тұрғысынан жоғары назарды қажет етсе.

2.7. Санкциялар

Санкциялар — мемлекеттер, халықаралық ұйымдар, құзыретті органдар белгілеген немесе Компания серіктестері арқылы қолданылатын экономикалық, қаржылық, сауда, жеке, аумақтық немесе өзге де шектеу шаралары.

2.8. Тыйым салынған юрисдикция

Тыйым салынған юрисдикция — заң, санкциялар, жоғары AML-тәуекел, серіктестер талаптары, ішкі тәуекелдерді басқару қағидалары немесе өзге жағдайлар себебінен Компания қызмет көрсетуді шектейтін немесе тыйым салатын ел, аумақ немесе өңір.

Тыйым салынған юрисдикциялар тізімі міндетті түрде осы Саясатта жарияланбайды және Платформа интерфейсінде, Компанияның ішкі қағидаларында, серіктестер құжаттарында немесе бөлек хабарламаларда айқындалуы мүмкін.

2.9. Күдікті белсенділік

Күдікті белсенділік — ақшаны жылыстатуды, терроризмді қаржыландыруды, санкцияларды айналып өтуді, алаяқтықты, скамды, бөтен деректерді пайдалануды, мультиаккаунтингті, заңсыз қызметті немесе өзге де қолайсыз тәуекелді көрсетуі мүмкін операция, мінез-құлық, қаражат көзі, P2P-мәміле, мекенжай, төлем әдісі, аккаунт немесе өзге фактор.

2.10. Red flags / қызыл жалаушалар

Red flags — жоғары тәуекелді немесе қосымша тексеру қажеттігін көрсетуі мүмкін белгілер немесе индикаторлар.

3. AML/KYC бақылауын ұйымдастыру

3.1. Жауапты тұлғалар

Компания AML/KYC рәсімдерін іске асыруға, тәуекелдерді басқаруға, транзакцияларды мониторингтеуге, күдікті белсенділікті қарауға, құзыретті

органдармен өзара іс-қимыл жасауға және ішкі қағидаларды қолдауға жауапты тұлғаны немесе командаңы тағайындай алады.

3.2. Ішкі қағидалар

Компания ішкі қағидаларды, нұсқаулықтарды, тәуекел критерийлерін, red flags, тексеру рәсімдерін, лимиттерді, мониторинг сценарийлерін және шешім қабылдау қағидаларын әзірлейді және қолданады.

Мұндай ішкі құжаттар Компанияның құпия ақпараты болып табылады және егер ашып көрсету бақылау тиімділігіне, Платформа қауіпсіздігіне, заңның орындалуына, үшінші тұлғалардың құқықтарына немесе тергеу мүдделеріне зиян келтіруі мүмкін болса, пайдаланушыларға ашып көрсетілмейді.

3.3. Рәсімдерді жаңарту

Компания AML/KYC рәсімдерін келесілерді ескере отырып жаңарта алады:

- заңнамадағы өзгерістер;
- жаңа өнімдер мен функциялар;
- алаяқтықтың жаңа схемалары;
- FATF ұсынымдары және өзге халықаралық стандарттар;
- серіктестер талаптары;
- ішкі тексерулер нәтижелері;
- қауіпсіздік инциденттері;
- санкциялық режимдердегі өзгерістер;
- ақшаны жылыстату және терроризмді қаржыландырудың жаңа типологиялары.

4. Тәуекелдерді бағалау

4.1. Жалпы тәуекелдерді бағалау

Компания Платформаға, пайдаланушыларға, өнімдерге, цифрлық активтерге, юрисдикцияларға, қол жеткізу арналарына, P2P-мәмілелерге, төлем әдістеріне, P2P-тен тыс фиат операцияларына, блокчейн-желілерге және қызмет жеткізушілерге байланысты AML/KYC-тәуекелдеріне тұрақты бағалау жүргізе алады.

4.2. Тәуекел факторлары

Тәуекелді бағалау кезінде Компания мыналарды ескеруі мүмкін:

- пайдаланушының тұратын елі, азаматтығы, орналасқан жері немесе IP-географиясы;
- аккаунт түрі және тіркелу тәсілі;
- операциялар тарихы;
- операциялардың сомалары мен жиілігі;
- пайдаланылатын цифрлық активтер мен желілер;
- жіберушілер мен алушылардың блокчейн-мекенжайлары;
- мекенжайлардың миксерлермен, даркнет-нарықтармен, бұзулармен, ransomware, скам-жобалармен, санкциялық мекенжайлармен немесе өзге жоғары тәуекелді көздермен байланысы;

- P2P-мәмілелерді пайдалану;
- таңдалған фиат төлем әдістері;
- даулардағы мінез-құлық;
- басқа пайдаланушылардың шағымдары;
- мультиаккаунтинг немесе бұрын бұғатталған аккаунттармен байланыс;
- VPN, прокси немесе орналасқан жерді жасыратын өзге құралдарды пайдалану;
- ақпарат беруден бас тарту;
- деректердің қайшылығы;
- PEP-мәртебе;
- санкциялық сәйкестіктер;
- adverse media және өзге беделдік факторлар;
- серіктестер мен құзыретті органдардың талаптары.

4.3. Тәуекел санаттары

Компания пайдаланушыларға, операцияларға, мекенжайларға немесе мәмілелерге төмен, орташа, жоғары немесе қолайсыз тәуекел сияқты ішкі тәуекел санаттарын тағайындай алады.

Тәуекел санаты мыналарға әсер етуі мүмкін:

- қолжетімді функциялар;
- лимиттер;
- KYC қажеттілігі;
- EDD қажеттілігі;
- операцияларды өңдеу жылдамдығы;
- шығару мүмкіндігі;
- P2P-ке қолжетімділік;
- қолмен тексеру қажеттілігі;
- мұздату немесе қызмет көрсетуден бас тарту ықтималдығы.

Компания пайдаланушыға ішкі тәуекел санатын, есептеу әдістемесін, нақты критерийлерді немесе скоринг нәтижелерін ашуға міндетті емес.

5. KYC/CDD: пайдаланушыларды тексеру

5.1. Жалпы тәсіл

Егер заңда, интерфейсте, серіктестер талаптарында немесе нақты функцияда өзгеше көзделмесе, Компания әдепкі бойынша барлық пайдаланушылардан толық KYC-верификацияны талап етпейді. Тексеру тәуекелге негізделген негізде қолданылады.

5.2. KYC қашан қажет болуы мүмкін

Компания келесі жағдайларда KYC немесе қосымша мәліметтерді сұрата алады:

- лимиттерге жету;

- ірі операция;
- әдеттен тыс операция;
- күдікті белсенділік;
- дау ашу;
- шығару сұрауы;
- мекенжай немесе транзакция бойынша AML-сәйкестік;
- жоғары тәуекелді юрисдикциямен байланыс;
- P2P-тен тыс фиат функциясын пайдалану;
- төлем серіктесінің, банктің, айырбастау провайдерінің немесе AML/KYC-провайдердің талабы;
- құзыретті органның сұрауы;
- аккаунтқа қол жеткізуді қалпына келтіру;
- мультиаккаунтингке, алаяқтыққа немесе бөтен деректерді пайдалануға күдік;
- тексеруді талап ететін өзге жағдайлар.

5.3. Қандай деректер сұратылуы мүмкін

Тәуекел деңгейіне байланысты Компания мыналарды сұрата алады:

- аты, тегі, әкесінің аты немесе өзге толық аты-жөні;
- туған күні;
- азаматтығы;
- тұратын елі;
- тұрғылықты мекенжайы;
- email;
- телефон нөмірі;
- жеке басын куәландыратын құжат;
- фотосурет, селфи, бейне-тексеру немесе liveness-тексеру;
- мекенжайды растау;
- қаражат көзін растау;
- байлық көзін растау;
- операция мақсатын растау;
- үзінді көшірме, чек, түбіртек немесе төлемді растау;
- P2P-мәміле бойынша құжаттар;
- PEP-пен байланыс туралы мәліметтер;
- тәуекелді бағалау үшін қажетті өзге құжаттар немесе түсіндірмелер.

5.4. Деректерді тексеру

Компания ұсынылған деректерді келесі түрде тексере алады:

- қолмен;
- автоматтандырылған жүйелерді пайдалану арқылы;
- сыртқы AML/KYC-провайдерлер арқылы;

- санкциялық және PEP-тізімдер арқылы;
- ашық дереккөздер арқылы;
- блокчейн-аналитика арқылы;
- серіктестерден, пайдаланушылардан, банктерден, төлем провайдерлерінен немесе құзыретті органдардан алынған ақпарат арқылы.

5.5. Пайдаланушының ынтымақтасу міндеті

Пайдаланушы сұратылған ақпарат пен құжаттарды уақтылы, дұрыс және толық беруге міндетті.

Егер пайдаланушы деректерді беруден бас тартса, жалған немесе қайшы мәліметтер берсе, сұрауларға жауап бермесе немесе тексеруді айналып өтуге тырысса, Компания функцияларды шектеуге, операцияларды тоқтата тұруға, активтерді мұздатуға, мәмілелерді жоюға, қызмет көрсетуден бас тартуға немесе аккаунтты жабуға құқылы.

5.6. Қайта тексеру

Пайдаланушы бұрын тексеруден өткен болса да, Компания құжаттарды немесе мәліметтерді қайта сұратуға құқылы, егер:

- пайдаланушы деректері өзгерсе;
- құжаттың қолданылу мерзімі аяқталса;
- пайдаланушының белсенділігі өзгерсе;
- жаңа тәуекелдер пайда болса;
- пайдаланушы жаңа лимиттерге жетсе;
- жаңа функция ашылса;
- заң немесе серіктестер талаптары өзгерсе;
- дау немесе күдікті белсенділік туындаса.

6. Күшейтілген тексеру EDD

6.1. EDD қашан қолданылады

Егер пайдаланушы, операция, мекенжай, P2P-мәміле, юрисдикция немесе мінез-құлық жоғары тәуекелге ие болса, Компания EDD қолдана алады.

EDD, атап айтқанда, келесі жағдайларда қолданылуы мүмкін:

- пайдаланушы PEP болса немесе PEP-пен байланысты болса;
- пайдаланушы жоғары тәуекелді юрисдикциямен байланысты болса;
- операция ірі, күрделі, әдеттен тыс немесе экономикалық тұрғыдан түсіндірілмейтін болса;
- қаражат жоғары тәуекелді блокчейн-мекенжайдан түссе;
- операция миксерлермен, даркнет-нарықтармен, бұзулармен, ransomware, скаммен, санкциялық мекенжайлармен немесе өзге қызыл жалаушалармен байланысты болса;
- пайдаланушы дауларды жиі ашса немесе жиі жеңілсе;
- мультиаккаунтинг белгілері болса;

- бөтен реквизиттерді немесе бөтен аккаунтты пайдалану белгілері болса;
- пайдаланушы қаражат көзін түсіндіре алмаса;
- пайдаланушы сұрақтарға қайшы жауап берсе;
- серіктес немесе құзыретті орган сұрауы бойынша растау қажет болса.

6.2. EDD шаралары

EDD мыналарды қамтуы мүмкін:

- қосымша құжаттарды сұрату;
- қаражат көзін растау;
- байлық көзін растау;
- операция мақсатын растау;
- ашық дереккөздерді тексеру;
- adverse media тексеруі;
- блокчейн-тарихты терең талдау;
- лимиттерді төмендету;
- қаражатты уақытша мұздату;
- операцияны қолмен келісу;
- операциядан бас тарту;
- қызмет көрсетуді тоқтату.

6.3. EDD нәтижелері

EDD нәтижелері бойынша Компания:

- операцияға рұқсат бере алады;
- операцияға лимиттермен немесе шарттармен рұқсат бере алады;
- қосымша мәліметтер сұрата алады;
- операциядан бас тарта алады;
- егер бұл рұқсат етілсе және мүмкін болса, қаражатты қайтара алады;
- қаражатты мұздата алады;
- аккаунтты шектей алады;
- аккаунтты жаба алады;
- егер заң талап етсе немесе рұқсат етсе, ақпаратты құзыретті органдарға бере алады.

7. KYT және транзакцияларды мониторингтеу

7.1. Жалпы мониторинг

Компания пайдаланушылар операцияларына тұрақты немесе таңдаулы мониторинг жүргізе алады, соның ішінде:

- цифрлық активтермен толықтырулар;
- цифрлық активтерді шығару;
- ішкі аударымдар;

- P2P-мәмілелер;
- егер мұндай функциялар қолжетімді болса, P2P-тен тыс фиат операциялары;
- операция жасау әрекеттері;
- жойылған операциялар;
- даулармен немесе шағымдармен байланысты операциялар.

7.2. Блокчейн-аналитика

Компания мекенжайлардың, транзакциялардың, мекенжай кластерлерінің, қаражат көздерінің және байланысты субъектілердің тәуекелін бағалау үшін блокчейн-аналитиканы пайдалана алады.

Тексеру келесілермен байланысты ескеруі мүмкін:

- санкциялық мекенжайлар;
- даркнет-нарықтар;
- миксерлер және обфускация сервистері;
- ransomware;
- бұзулар және ұрланған қаражат;
- скам-жобалар;
- алаяқтық схемалар;
- заңсыз сервистер;
- жоғары тәуекелді биржалар немесе айырбастаушылар;
- жоғары тәуекелдің өзге көздері.

7.3. P2P-мониторинг

P2P-мәмілелерде Компания мыналарды талдай алады:

- мәмілелер жиілігі;
- мәмілелер сомалары;
- тараптардың мінез-құлқы;
- жоюлар саны;
- даулар саны;
- шағымдар;
- төлемді растаулар;
- реквизиттердің сәйкестігі;
- аккаунттар байланысы;
- мультиаккаунтинг белгілері;
- төлем деректерінің сәйкессіздігі;
- мәмілені Платформа қағидаларынан тыс шығару әрекеттері;
- бөтен банк шоттарын, карталарын немесе төлем реквизиттерін пайдалану.

7.4. Лимиттер және кідірістер

Компания жекелеген пайдаланушылар, операциялар, мәмілелер, мекенжайлар, активтер, төлем әдістері немесе юрисдикциялар үшін лимиттер, кідірістер, қолмен

тексерулер немесе қосымша талаптар белгілей алады.

Операция тексеру аяқталғанға дейін кідіртілуі немесе тоқтатыла тұруы мүмкін.

8. Red flags: күдікті белсенділік белгілері

Red flags қатарына, атап айтқанда, мыналар кіруі мүмкін:

- пайдаланушының деректерді немесе құжаттарды беруден бас тартуы;
- жалған, өзгертілген немесе қайшы құжаттарды ұсыну;
- бөтен деректерді, бөтен карталарды, бөтен шоттарды немесе бөтен әмияндарды пайдалану;
- бірнеше аккаунт пайдалануға әрекет жасау;
- P2P-мәмілелерді жиі жою;
- P2P-мәмілелер бойынша жиі даулар;
- жалған чектер, түбіртектер немесе төлем скриншоттары;
- төлеушінің аты мен пайдаланушының сәйкес келмеуі;
- айқын экономикалық мақсатсыз қаражатты жылдам енгізу және шығару;
- операцияларды бірнеше ұсақ сомаға құрылымдау;
- пайдаланушының әдеттегі мінез-құлқына сәйкес келмейтін операциялар;
- жоғары тәуекелді блокчейн-мекенжайларды пайдалану;
- миксерлермен, даркнет-нарықтармен, бұзулармен, ransomware, скаммен немесе санкциялық мекенжайлармен байланыс;
- айналымның күрт өсуі;
- лимиттерді айналып өту әрекеттері;
- шектеулерді айналып өту үшін VPN, прокси немесе орналасқан жерді жасыратын өзге құралдарды пайдалану;
- контрагентке немесе қолдауға агрессивті қысым көрсету;
- қаражат көзін түсіндіруден бас тарту;
- мәмілені Платформадан тыс шығаруға әрекет жасау;
- басқа пайдаланушылардың шағымдары;
- ашық дереккөздерден теріс ақпарат;
- санкциялық, PEP немесе adverse media көздерімен сәйкестік.

Бір red flag болуы әрқашан бұзушылықты білдірмейді, бірақ қосымша тексеруге, операцияны шектеуге немесе өзге шараларға негіз болуы мүмкін.

9. Санкциялар және тыйым салынған қатынастар

Егер бұл заңмен, санкциялармен, серіктестер талаптарымен немесе ішкі тәуекелдерді басқару қағидаларымен тыйым салынса, Компания пайдаланушылармен қатынас орнатпайды және жалғастырмайды.

Компания қызмет көрсетуден бас тарта алады, аккаунтты шектей алады, активтерді мұздата алады немесе қатынастарды тоқтата алады, егер пайдаланушы:

- санкциялық тізімде болса;
- санкциялық тізімдегі тұлғамен байланысты болса;
- тыйым салынған юрисдикцияда болса;
- тыйым салынған тұлғаның мүддесі үшін әрекет етсе;
- Платформаны санкцияларды айналып өту үшін пайдаланса;
- санкциялық тексеру үшін қажетті ақпаратты беруден бас тартса.

Компания тіркеу кезінде, операция алдында, операциядан кейін, санкциялық тізімдер өзгерген кезде, дау ашылған кезде, қаражат шығарылған кезде немесе өзге жағдайларда санкциялық тексерулер жүргізе алады.

10. Тыйым салынған қызмет

Пайдаланушыға Платформаны келесі мақсаттарда пайдалануға тыйым салынады:

- ақшаны жылыстату;
- терроризмді қаржыландыру;
- санкцияларды айналып өту;
- алаяқтық, скам, фишинг немесе әлеуметтік инженерия;
- ұрланған қаражатпен, аккаунттармен, карталармен, құжаттармен немесе дербес деректермен сауда жасау;
- заңды негізсіз бөтен банк карталарын, шоттарын, әмияндарын немесе реквизиттерін пайдалану;
- есірткі, қару, қауіпті заттар немесе өзге тыйым салынған тауарлардың заңсыз айналымы;
- заңсыз құмар ойындар;
- заңсыз қаржылық қызметтер;
- даркнет-қызмет;
- экстремистік, террористік немесе өзге тыйым салынған қызметті қаржыландыру;
- үшінші тұлғалардың құқықтарын бұзу;
- жалған құжаттарды, чектерді, түбіртектерді немесе скриншоттарды пайдалану;
- мультиаккаунтинг және шектеулерді айналып өту;
- Компания заңсыз, жоғары тәуекелді немесе қолайсыз деп санайтын өзге қызмет.

11. Тәуекел анықталған кездегі Компания шаралары

Егер Компания күдікті белсенділікті, AML/KYC-тәуекелді, санкциялық тәуекелді, осы Саясаттың бұзылуын немесе пайдаланушының ынтымақтасудан бас тартуын анықтаса, Компания:

- қосымша мәліметтер сұрата алады;
- KYC немесе EDD сұрата алады;
- лимиттерді төмендете алады;
- операцияны кідірте алады;
- операциядан бас тарта алады;

- P2P-мәмілені жоя алады;
- P2P-функцияларды шектей алады;
- активтерді мұздата немесе резервтей алады;
- шығаруды шектей алады;
- аккаунтты уақытша бұғаттай алады;
- аккаунтты жаба алады;
- егер бұл мүмкін, рұқсат етілген және заңмен тыйым салынбаған болса, қаражатты жіберушіге қайтара алады;
- егер бұл Платформа қағидаларында көзделсе, қолданылатын комиссияларды, желілік шығындарды немесе қайтару шығындарын ұстап қала алады;
- егер заң талап етсе немесе рұқсат етсе, ақпаратты құзыретті органдарға бере алады;
- Платформаны, пайдаланушыларды, серіктестерді және Компанияны қорғау үшін өзге де ақылға қонымды шаралар қолдана алады.

Егер хабарлау заңды, AML/KYC/CTF талаптарын, санкциялық қағидаларды, тергеу мүдделерін, Платформа қауіпсіздігін немесе үшінші тұлғалардың құқықтарын бұзуы мүмкін болса, Компания мұндай шараларды қолдану туралы пайдаланушыны алдын ала хабардар етуге міндетті емес.

12. AML/KYC-бас тарту кезіндегі қаражатты қайтару

Егер операция AML/KYC-тексеру нәтижелері бойынша қабылданбаса немесе қызмет көрсету шектелсе, Компания мүмкін және рұқсат етілген жағдайда цифрлық активтерді жіберушінің бастапқы мекенжайына немесе Компания тәуекел және заң тұрғысынан қолайлы деп санайтын өзге мекенжайға қайтара алады.

Қайтару мүмкін болмауы немесе кейінге қалдырылуы мүмкін, егер:

- қаражат санкциялық мекенжаймен байланысты болса;
- қаражат қылмыстық қызметпен байланысты болса;
- құзыретті органнан сұрау алынса;
- қайтару заңды бұзуы мүмкін болса;
- бастапқы мекенжай қолжетімсіз, жоғары тәуекелді немесе техникалық тұрғыдан жарамсыз болса;
- қосымша тексеру қажет болса;
- қаражат бұрыннан резервтелген, мұздатылған немесе даумен байланысты болса.

Қайтару сомасынан желілік комиссиялар, сервистік комиссиялар, өңдеу шығындары және өзге қолданылатын шығындар ұсталып қалуы мүмкін, егер олар Пайдалану шарттарында, https://kashbi.io/information/fees комиссиялар бетінде, Платформа интерфейсінде немесе бөлек қағидаларда көзделсе.

Мұндай қайтару үшін комиссияның немесе алымның нақты мөлшері осы Саясатта бекітілмейді және, егер мұндай алым қолданылса, https://kashbi.io/information/fees комиссиялар бетінде, Платформа интерфейсінде немесе бөлек қағидаларда айқындалуы мүмкін.

13. Есептілік және органдармен өзара іс-қимыл

Компания заңмен талап етілген немесе рұқсат етілген жағдайда құзыретті органдармен, қаржылық барлау бөлімшелерімен, құқық қорғау органдарымен, соттармен, реттеушілермен, банктермен, төлем провайдерлерімен және өзге уәкілетті тұлғалармен өзара іс-қимыл жасай алады.

Компания пайдаланушы, аккаунт, транзакция, P2P-мәміле, дау, мекенжай, төлем деректері немесе өзге жағдайлар туралы ақпаратты бере алады, егер:

- заңды сұрау алынса;
- күдікті белсенділік туралы хабарлау міндеті болса;
- санкциялық талаптарды орындау қажет болса;
- Компанияның, пайдаланушылардың немесе үшінші тұлғалардың құқықтарын қорғау қажет болса;
- алаяқтықтың, ақшаны жылыстатудың немесе терроризмді қаржыландырудың алдын алу қажет болса.

Егер хабарлау заңмен тыйым салынса, тергеуге кедергі келтіруі мүмкін болса, ішкі AML-рәсімдерді ашуы мүмкін болса немесе қауіпсіздік тәуекелін тудырса, Компания мұндай берілім туралы пайдаланушыны хабардар етуге міндетті емес.

14. Деректер мен жазбаларды сақтау

Компания AML/KYC, транзакциялар, P2P-мәмілелер, тексерулер, даулар, шектеулер және есептілікке байланысты деректер мен жазбаларды қолданылатын заңнамада, серіктестер талаптарында, ішкі тәуекелдерді басқару қағидаларында және Құпиялылық саясатында көзделген мерзім ішінде сақтайды.

Мұндай деректерге мыналар кіруі мүмкін:

- KYC-деректер;
- пайдаланушы құжаттары;
- тексеру нәтижелері;
- санкциялық және PEP-сәйкестіктер;
- тәуекел профилі;
- операциялар тарихы;
- блокчейн-мекенжайлар;
- транзакциялардың txid/hash;
- P2P-мәмілелер деректері;
- төлемді растаулар;
- даулар материалдары;
- қолдаумен хат алмасу;
- шектеулер бойынша ішкі шешімдер;
- құзыретті органдар сұраулары туралы жазбалар.

Аккаунтты жою, келісімді қайтарып алу немесе Платформаны пайдалануды тоқтату

AML/KYC-деректерін дереу жоюды әрқашан білдірмейді, егер оларды сақтау заңмен, AML/KYC/CTF қағидаларымен, Компания құқықтарын қорғаумен, дауларды шешумен немесе құзыретті органдар сұрауларын орындаумен талап етілсе немесе рұқсат етілсе.

15. Үшінші тұлғалар және қызмет жеткізушілер

Компания AML/KYC рәсімдерін орындау үшін үшінші тұлғаларды тарта алады, соның ішінде:

- құжаттарды тексеру жеткізушілері;
- liveness-тексеру жеткізушілері;
- санкциялық скрининг жеткізушілері;
- PEP/adverse media тексеру жеткізушілері;
- блокчейн-аналитика жеткізушілері;
- төлем серіктестері;
- банктер, процессингтер және айырбастау провайдерлері;
- құқықтық, комплаенс және аудиторлық консультанттар;
- инфрақұрылым және қауіпсіздік жеткізушілері.

Егер заң, провайдермен шарт немесе Компанияның бөлек саясаты өзгеше талап етпесе, провайдерлер нақты атауларсыз санаттар бойынша көрсетілуі мүмкін.

Компания серіктестер мен жеткізушілерді санкциялар, бедел, лицензиялар, рұқсаттар, тәуекелдер және қауіпсіздік пен құпиялылық талаптарын сақтау қабілеті тұрғысынан тексере алады.

16. Пайдаланушы міндеттері

Пайдаланушы міндеттенеді:

- Платформаны тыйым салынған қызмет үшін пайдаланбауға;
- дұрыс мәліметтер беруге;
- Компания сұрауларына уақтылы жауап беруге;
- егер сұратылса, құжаттар мен түсіндірмелер беруге;
- тек заңды түрде өзіне тиесілі қаражатты пайдалануға;
- заңды негізсіз бөтен банк карталарын, шоттарын, әмияндарын немесе реквизиттерін пайдаланбауға;
- жалған құжаттар, чектер, скриншоттар немесе түбіртектер ұсынбауға;
- лимиттерді, тексерулерді, санкциялық шектеулерді немесе Платформа қағидаларын айналып өтпеуге;
- шектеулерді айналып өту үшін бірнеше аккаунт жасамауға;
- қолданылатын заңнаманы сақтауға;
- өз операцияларының тұратын еліндегі заңдылығын дербес бағалауға.

Ынтымақтасудан бас тарту, тексеруден жалтару, жалған мәліметтер беру немесе AML/KYC-бақылауды айналып өту әрекеті қызмет көрсетуді шектеуге немесе

тоқтатуға әкелуі мүмкін.

17. AML/KYC рәсімдерінің құпиялылығы

Пайдаланушы Компания мыналарды ашпайтынын түсінеді:

- нақты тәуекел критерийлері;
- ішкі red flags;
- мониторинг шектері;
- скоринг алгоритмдері;
- AML-деректер көздері;
- тергеу мәліметтері;
- құзыретті органдарға есеп беру себептері;
- ішкі шешімдер мәліметтері;
- ашып көрсету заңды, қауіпсіздікті немесе AML/KYC-бақылау тиімділігін бұзуы мүмкін ақпарат.

18. Саясатты өзгерту

Компания осы Саясатты кез келген уақытта өзгерте алады. Өзекті нұсқа https://kashbi.io сайтында немесе Платформа интерфейсінде жарияланады.

Жаңартылған нұсқа жарияланғаннан кейін Платформаны пайдалануды жалғастыру, егер қолданылатын заңнамада өзгеше көзделмесе, пайдаланушының Саясаттың жаңа редакциясымен келісетінін білдіреді.

19. Тілдік нұсқалар

Осы Саясат орыс, қазақ, ағылшын және өзге тілдерде жариялануы мүмкін.

Егер қолданылатын заңнама белгілі бір тілдік нұсқаның басымдығын талап етсе, сол нұсқа қолданылады. Қалған жағдайларда тілдік нұсқалар арасында сәйкессіздіктер болған жағдайда, орыс тіліндегі нұсқа басым болады.

20. Байланыстар

Осы Саясат бойынша сұрақтар туындаған жағдайда пайдаланушы келесі байланыстар арқылы жүгіне алады:

- Компания: F-Tech
- Тіркелген елі: Kazakhstan
- Сайт: https://kashbi.io
- Қолданба: KashBi
- Email: legal@kashbi.io
- Telegram: kashbi_support
- Заңды мекенжай: 44/1 Al-Farabi Avenue, Apartment 207