Політика AML/KYC

Ця Політика AML/KYC («Політика») описує підхід F-Tech, зареєстрованої в Kazakhstan («Компанія», «ми», «нас», «наш»), до запобігання відмиванню доходів, фінансуванню тероризму, обходу санкцій, шахрайству та іншій незаконній або забороненій діяльності під час використання сайту https://kashbi.io, застосунку KashBi, Telegram-бота, Telegram Mini App, web-версії, API, крипто-фіатного гаманця, P2P-платформи та інших пов’язаних сервісів Компанії, спільно іменованих «Платформа».

Ця Політика є частиною Умов користування та застосовується разом із Політикою конфіденційності, правилами P2P-угод, правилами комісій, попередженнями про ризики та іншими документами Компанії.

Використовуючи Платформу, створюючи акаунт, поповнюючи баланс, виводячи цифрові активи, створюючи або приймаючи P2P-угоду, проходячи перевірку або іншим чином взаємодіючи з Платформою, користувач підтверджує, що ознайомився з цією Політикою та погоджується дотримуватися її положень.

Якщо користувач не погоджується з цією Політикою, він повинен припинити використання Платформи.

1. Мета та сфера застосування

1.1. Мета Політики

Мета цієї Політики — встановити основні принципи, правила та заходи, спрямовані на:

- запобігання використанню Платформи для відмивання доходів;
- запобігання фінансуванню тероризму;
- запобігання обходу санкцій;
- запобігання шахрайству, скаму, фішингу та іншій протиправній діяльності;
- виявлення та оцінку високоризикових користувачів, операцій, адрес і юрисдикцій;
- моніторинг операцій із цифровими активами та P2P-угод;
- виконання застосовних вимог законодавства, вимог партнерів, постачальників AML/KYC-сервісів, банків, платіжних провайдерів і компетентних органів;
- захист користувачів, Компанії, Платформи та її ділової репутації.

1.2. Сфера застосування

Ця Політика застосовується до всіх користувачів Платформи, включно з користувачами:

- крипто-фіатного гаманця;
- P2P-платформи;
- Telegram Mini App;
- Telegram-бота;

- web-версії;
- функцій поповнення та виведення цифрових активів;
- внутрішніх переказів;
- фіатних операцій поза P2P, якщо такі функції доступні;
- служби підтримки та спорів.

1.3. Risk-based підхід

Компанія застосовує ризик-орієнтований підхід. Це означає, що KYC, AML-перевірки, ліміти, запити документів, посилена перевірка, моніторинг, обмеження та інші заходи застосовуються пропорційно рівню ризику користувача, операції, юрисдикції, платіжного методу, цифрового активу, блокчейн-адреси, поведінки користувача та інших факторів.

Платформа позиціонується як privacy-first: Компанія прагне мінімізувати збір персональних даних і не запитувати ідентифікаційні документи без необхідності. Водночас privacy-first не означає повну анонімність і не виключає обробку даних, перевірку користувача, перевірку транзакцій, обмеження операцій або передачу інформації компетентним органам, якщо це вимагається або допускається законом, правилами Платформи, вимогами партнерів або цією Політикою.

2. Терміни та визначення

2.1. AML

AML — заходи з протидії відмиванню доходів, отриманих злочинним шляхом, включно з виявленням, запобіганням, розслідуванням та обмеженням операцій, пов’язаних із незаконним походженням коштів.

2.2. KYC

KYC — процедура «знай свого клієнта», що включає ідентифікацію, перевірку та оцінку користувача, якщо така процедура потрібна з урахуванням ризику, лімітів, операції, застосовного законодавства або вимог партнерів.

2.3. CDD

CDD — належна перевірка клієнта, що включає збір та аналіз інформації про користувача, його активність, джерело коштів, цілі операцій і профіль ризику.

2.4. EDD

EDD — посилена перевірка клієнта, що застосовується до користувачів, операцій або ситуацій підвищеного ризику. EDD може включати запит додаткових документів, підтвердження джерела коштів, розширений аналіз транзакцій, перевірку відкритих джерел, санкційні та PEP-перевірки, а також погодження подальшого обслуговування на рівні відповідальних осіб Компанії.

2.5. KYT

KYT — процедура «знай свою транзакцію», що включає аналіз операцій, блокчейн-адрес, джерел коштів, поведінки користувача, пов’язаних гаманців, P2P-патернів та інших даних, що стосуються конкретної операції.

2.6. PEP

PEP — політично значуща особа, а також члени її сім’ї та особи, тісно пов’язані з такою особою, якщо такі особи потребують підвищеної уваги з точки зору корупційних, санкційних, репутаційних або інших ризиків.

2.7. Санкції

Санкції — економічні, фінансові, торговельні, персональні, територіальні або інші обмежувальні заходи, встановлені державами, міжнародними організаціями, компетентними органами або застосовні через партнерів Компанії.

2.8. Заборонена юрисдикція

Заборонена юрисдикція — країна, територія або регіон, щодо яких Компанія обмежує або забороняє обслуговування через закон, санкції, високий AML-ризик, вимоги партнерів, внутрішні правила управління ризиками або інші обставини.

Перелік заборонених юрисдикцій не обов’язково публікується в цій Політиці та може визначатися в інтерфейсі Платформи, внутрішніх правилах Компанії, документах партнерів або окремих повідомленнях.

2.9. Підозріла активність

Підозріла активність — операція, поведінка, джерело коштів, P2P-угода, адреса, платіжний метод, акаунт або інший фактор, який може вказувати на відмивання доходів, фінансування тероризму, обхід санкцій, шахрайство, скам, використання чужих даних, мультиакаунтинг, незаконну діяльність або інший неприйнятний ризик.

2.10. Red flags / червоні прапорці

Red flags — ознаки або індикатори, які можуть вказувати на підвищений ризик або необхідність додаткової перевірки.

3. Організація AML/KYC-контролю

3.1. Відповідальні особи

Компанія може призначати відповідальну особу або команду, відповідальну за реалізацію AML/KYC-процедур, управління ризиками, моніторинг транзакцій, розгляд підозрілої активності, взаємодію з компетентними органами та підтримання внутрішніх правил.

3.2. Внутрішні правила

Компанія розробляє та застосовує внутрішні правила, інструкції, критерії ризику, red flags, процедури перевірки, ліміти, сценарії моніторингу та правила ухвалення рішень.

Такі внутрішні документи є конфіденційною інформацією Компанії та не підлягають розкриттю користувачам, якщо розкриття може зашкодити ефективності контролю, безпеці Платформи, виконанню закону, правам третіх осіб або інтересам розслідування.

3.3. Оновлення процедур

Компанія може оновлювати AML/KYC-процедури з урахуванням:

- змін законодавства;
- нових продуктів і функцій;
- нових схем шахрайства;
- рекомендацій FATF та інших міжнародних стандартів;
- вимог партнерів;
- результатів внутрішніх перевірок;
- інцидентів безпеки;
- змін санкційних режимів;
- нових типологій відмивання доходів і фінансування тероризму.

4. Оцінка ризиків

4.1. Загальна оцінка ризиків

Компанія може проводити регулярну оцінку AML/KYC-ризиків, пов’язаних із Платформою, користувачами, продуктами, цифровими активами, юрисдикціями, каналами доступу, P2P-угодами, платіжними методами, фіатними операціями поза P2P, блокчейн-мережами та постачальниками послуг.

4.2. Фактори ризику

Під час оцінки ризику Компанія може враховувати:

- країну проживання, громадянство, місцезнаходження або IP-географію користувача;
- тип акаунта та спосіб реєстрації;
- історію операцій;
- суми та частоту операцій;
- використовувані цифрові активи та мережі;
- блокчейн-адреси відправників і отримувачів;
- зв’язок адрес із міксерами, даркнет-ринками, зламами, ransomware, скам-проєктами, санкційними адресами або іншими високоризиковими джерелами;
- використання P2P-угод;
- обрані фіатні платіжні методи;
- поведінку в спорах;
- скарги інших користувачів;
- мультиакаунтинг або зв’язок із раніше заблокованими акаунтами;
- використання VPN, проксі або інших засобів приховування місцезнаходження;
- відмову від надання інформації;
- суперечливість даних;
- PEP-статус;
- санкційні збіги;

- adverse media та інші репутаційні фактори;
- вимоги партнерів і компетентних органів.

4.3. Категорії ризику

Компанія може присвоювати користувачам, операціям, адресам або угодам внутрішні категорії ризику, наприклад низький, середній, високий або неприйнятний ризик.

Категорія ризику може впливати на:

- доступні функції;
- ліміти;
- необхідність KYC;
- необхідність EDD;
- швидкість обробки операцій;
- можливість виведення;
- доступ до P2P;
- необхідність ручної перевірки;
- імовірність заморожування або відмови в обслуговуванні.

Компанія не зобов’язана розкривати користувачу внутрішню категорію ризику, методику розрахунку, точні критерії або результати скорингу.

5. KYC/CDD: перевірка користувачів

5.1. Загальний підхід

Компанія не вимагає повної KYC-верифікації від усіх користувачів за замовчуванням, якщо інше не передбачено законом, інтерфейсом, вимогами партнерів або конкретною функцією. Перевірка застосовується на ризик-орієнтованій основі.

5.2. Коли може знадобитися KYC

Компанія може запросити KYC або додаткові відомості у таких випадках:

- досягнення лімітів;
- велика операція;
- незвична операція;
- підозріла активність;
- відкриття спору;
- запит на виведення;
- AML-збіг за адресою або транзакцією;
- зв’язок із високоризиковою юрисдикцією;
- використання фіатної функції поза P2P;
- вимога платіжного партнера, банку, обмінного провайдера або AML/KYC-провайдера;
- запит компетентного органу;

- відновлення доступу до акаунта;
- підозра на мультиакаунтинг, шахрайство або використання чужих даних;
- інші обставини, що потребують перевірки.

5.3. Які дані можуть запитуватися

Залежно від рівня ризику Компанія може запросити:

- ім’я, прізвище, по батькові або інше повне ім’я;
- дату народження;
- громадянство;
- країну проживання;
- адресу проживання;
- email;
- номер телефону;
- документ, що посвідчує особу;
- фотографію, селфі, відеоперевірку або liveness-перевірку;
- підтвердження адреси;
- підтвердження джерела коштів;
- підтвердження джерела статків;
- підтвердження мети операції;
- виписку, чек, квитанцію або підтвердження платежу;
- документи щодо P2P-угоди;
- відомості про зв’язок із PEP;
- інші документи або пояснення, необхідні для оцінки ризику.

5.4. Перевірка даних

Компанія може перевіряти надані дані:

- вручну;
- з використанням автоматизованих систем;
- через зовнішніх AML/KYC-провайдерів;
- через санкційні та PEP-списки;
- через відкриті джерела;
- через блокчейн-аналітику;
- через інформацію, отриману від партнерів, користувачів, банків, платіжних провайдерів або компетентних органів.

5.5. Обов’язок користувача співпрацювати

Користувач зобов’язаний своєчасно, достовірно та повно надавати запитувану інформацію і документи.

Якщо користувач відмовляється надати дані, надає неправдиві або суперечливі відомості, не відповідає на запити або намагається обійти перевірку, Компанія має право обмежити функції, призупинити операції, заморозити активи, скасувати

угоди, відмовити в обслуговуванні або закрити акаунт.

5.6. Повторна перевірка

Компанія має право повторно запросити документи або відомості, навіть якщо користувач раніше вже проходив перевірку, якщо:

- змінилися дані користувача;
- закінчився строк дії документа;
- змінилася активність користувача;
- з’явилися нові ризики;
- користувач досяг нових лімітів;
- відкрилася нова функція;
- змінилися вимоги закону або партнерів;
- виник спір або підозріла активність.

6. Посилена перевірка EDD

6.1. Коли застосовується EDD

Компанія може застосувати EDD, якщо користувач, операція, адреса, P2P-угода, юрисдикція або поведінка має підвищений ризик.

EDD може застосовуватися, зокрема, якщо:

- користувач є PEP або пов’язаний із PEP;
- користувач пов’язаний із високоризиковою юрисдикцією;
- операція є великою, складною, незвичною або економічно незрозумілою;
- кошти надходять із високоризикової блокчейн-адреси;
- операція пов’язана з міксерами, даркнет-ринками, зламами, ransomware, скамом, санкційними адресами або іншими червоними прапорцями;
- користувач часто відкриває або програє спори;
- є ознаки мультиакаунтингу;
- є ознаки використання чужих реквізитів або чужого акаунта;
- користувач не може пояснити джерело коштів;
- користувач суперечливо відповідає на запитання;
- потрібне підтвердження на запит партнера або компетентного органу.

6.2. Заходи EDD

EDD може включати:

- запит додаткових документів;
- підтвердження джерела коштів;
- підтвердження джерела статків;
- підтвердження мети операції;
- перевірку відкритих джерел;
- перевірку adverse media;

- поглиблений аналіз блокчейн-історії;
- зниження лімітів;
- тимчасове заморожування коштів;
- ручне погодження операції;
- відмову в операції;
- припинення обслуговування.

6.3. Результати EDD

За результатами EDD Компанія може:

- дозволити операцію;
- дозволити операцію з лімітами або умовами;
- запросити додаткові відомості;
- відмовити в операції;
- повернути кошти, якщо це допустимо і можливо;
- заморозити кошти;
- обмежити акаунт;
- закрити акаунт;
- передати інформацію компетентним органам, якщо це вимагається або допускається законом.

7. KYT і моніторинг транзакцій

7.1. Загальний моніторинг

Компанія може здійснювати постійний або вибірковий моніторинг операцій користувачів, включно з:

- поповненнями цифровими активами;
- виведеннями цифрових активів;
- внутрішніми переказами;
- P2P-угодами;
- фіатними операціями поза P2P, якщо такі функції доступні;
- спробами операцій;
- скасованими операціями;
- операціями, пов’язаними зі спорами або скаргами.

7.2. Блокчейн-аналітика

Компанія може використовувати блокчейн-аналітику для оцінки ризику адрес, транзакцій, кластерів адрес, джерел коштів і пов’язаних сутностей.

Перевірка може враховувати зв’язок із:

- санкційними адресами;
- даркнет-ринками;
- міксерами і сервісами обфускації;

- ransomware;
- зламами та викраденими коштами;
- скам-проєктами;
- шахрайськими схемами;
- незаконними сервісами;
- високоризиковими біржами або обмінниками;
- іншими джерелами підвищеного ризику.

7.3. P2P-моніторинг

У P2P-угодах Компанія може аналізувати:

- частоту угод;
- суми угод;
- поведінку сторін;
- кількість скасувань;
- кількість спорів;
- скарги;
- підтвердження оплати;
- збіги реквізитів;
- зв’язок акаунтів;
- ознаки мультиакаунтингу;
- невідповідність платіжних даних;
- спроби вивести угоду за межі правил Платформи;
- використання чужих банківських рахунків, карт або платіжних реквізитів.

7.4. Ліміти та затримки

Компанія може встановлювати ліміти, затримки, ручні перевірки або додаткові вимоги для окремих користувачів, операцій, угод, адрес, активів, платіжних методів або юрисдикцій.

Операція може бути затримана або призупинена до завершення перевірки.

8. Red flags: ознаки підозрілої активності

До red flags можуть належати, зокрема:

- відмова користувача надати дані або документи;
- надання підроблених, змінених або суперечливих документів;
- використання чужих даних, чужих карт, чужих рахунків або чужих гаманців;
- спроба використовувати кілька акаунтів;
- часті скасування P2P-угод;
- часті спори щодо P2P-угод;
- підроблені чеки, квитанції або скриншоти оплати;
- невідповідність імені платника та користувача;

- швидке введення і виведення коштів без очевидної економічної мети;
- структурування операцій на кілька дрібних сум;
- операції, що не відповідають звичайній поведінці користувача;
- використання високоризикових блокчейн-адрес;
- зв’язок із міксерами, даркнет-ринками, зламами, ransomware, скамом або санкційними адресами;
- різке зростання обороту;
- спроби обійти ліміти;
- використання VPN, проксі або інших засобів приховування місцезнаходження для обходу обмежень;
- агресивний тиск на контрагента або підтримку;
- відмова пояснити джерело коштів;
- спроба вивести угоду за межі Платформи;
- скарги від інших користувачів;
- негативна інформація з відкритих джерел;
- збіг із санкційними, PEP або adverse media-джерелами.

Наявність одного red flag не завжди означає порушення, але може стати підставою для додаткової перевірки, обмеження операції або інших заходів.

9. Санкції та заборонені відносини

Компанія не встановлює і не продовжує відносини з користувачами, якщо це заборонено законом, санкціями, вимогами партнерів або внутрішніми правилами управління ризиками.

Компанія може відмовити в обслуговуванні, обмежити акаунт, заморозити активи або припинити відносини, якщо користувач:

- перебуває в санкційному списку;
- пов’язаний з особою із санкційного списку;
- перебуває в забороненій юрисдикції;
- діє в інтересах забороненої особи;
- використовує Платформу для обходу санкцій;
- відмовляється надати інформацію, необхідну для санкційної перевірки.

Компанія може проводити санкційні перевірки під час реєстрації, перед операцією, після операції, у разі зміни санкційних списків, під час відкриття спору, під час виведення коштів або в інших випадках.

10. Заборонена діяльність

Користувачу заборонено використовувати Платформу для:

- відмивання доходів;
- фінансування тероризму;
- обходу санкцій;

- шахрайства, скаму, фішингу або соціальної інженерії;
- торгівлі викраденими коштами, акаунтами, картами, документами або персональними даними;
- використання чужих банківських карт, рахунків, гаманців або реквізитів без законної підстави;
- незаконного обігу наркотиків, зброї, небезпечних речовин або інших заборонених товарів;
- незаконних азартних ігор;
- нелегальних фінансових послуг;
- даркнет-активності;
- фінансування екстремістської, терористичної або іншої забороненої діяльності;
- порушення прав третіх осіб;
- використання підроблених документів, чеків, квитанцій або скриншотів;
- мультиакаунтингу та обходу обмежень;
- іншої діяльності, яку Компанія вважає незаконною, високоризиковою або неприйнятною.

11. Заходи Компанії у разі виявлення ризику

Якщо Компанія виявляє підозрілу активність, AML/KYC-ризик, санкційний ризик, порушення цієї Політики або відмову користувача співпрацювати, Компанія має право:

- запросити додаткові відомості;
- запросити KYC або EDD;
- знизити ліміти;
- затримати операцію;
- відмовити в операції;
- скасувати P2P-угоду;
- обмежити P2P-функції;
- заморозити або зарезервувати активи;
- обмежити виведення;
- тимчасово заблокувати акаунт;
- закрити акаунт;
- повернути кошти відправнику, якщо це можливо, допустимо і не заборонено законом;
- утримати застосовні комісії, мережеві витрати або витрати на повернення, якщо це передбачено правилами Платформи;
- передати інформацію компетентним органам, якщо це вимагається або допускається законом;
- вжити інших розумних заходів для захисту Платформи, користувачів, партнерів і Компанії.

Компанія не зобов’язана заздалегідь повідомляти користувача про застосування

таких заходів, якщо повідомлення може порушити закон, вимоги AML/KYC/CTF, санкційні правила, інтереси розслідування, безпеку Платформи або права третіх осіб.

12. Повернення коштів у разі AML/KYC-відмови

Якщо операцію відхилено або обслуговування обмежено за результатами AML/KYC-перевірки, Компанія може, якщо це можливо і допустимо, повернути цифрові активи на вихідну адресу відправника або іншу адресу, яку Компанія вважатиме допустимою з точки зору ризику та закону.

Повернення може бути неможливим або відкладеним, якщо:

- кошти пов’язані із санкційною адресою;
- кошти пов’язані зі злочинною активністю;
- отримано запит компетентного органу;
- повернення може порушити закон;
- вихідна адреса недоступна, високоризикова або технічно непридатна;
- потрібна додаткова перевірка;
- кошти вже зарезервовані, заморожені або пов’язані зі спором.

Із суми повернення можуть утримуватися мережеві комісії, сервісні комісії, витрати на обробку та інші застосовні витрати, якщо вони передбачені Умовами користування, сторінкою комісій https://kashbi.io/information/fees, інтерфейсом Платформи або окремими правилами.

Конкретний розмір комісії або збору за таке повернення не фіксується в цій Політиці та може визначатися сторінкою комісій https://kashbi.io/information/fees, інтерфейсом Платформи або окремими правилами, якщо такий збір застосовується.

13. Звітність і взаємодія з органами

Компанія може взаємодіяти з компетентними органами, підрозділами фінансової розвідки, правоохоронними органами, судами, регуляторами, банками, платіжними провайдерами та іншими уповноваженими особами, якщо це вимагається або допускається законом.

Компанія може передавати інформацію про користувача, акаунт, транзакцію, P2P-угоду, спір, адресу, платіжні дані або інші обставини, якщо:

- отримано законний запит;
- існує обов’язок повідомити про підозрілу активність;
- потрібно виконати санкційні вимоги;
- необхідно захистити права Компанії, користувачів або третіх осіб;
- потрібно запобігти шахрайству, відмиванню доходів або фінансуванню тероризму.

Компанія не зобов’язана повідомляти користувача про таку передачу, якщо повідомлення заборонене законом, може завадити розслідуванню, розкрити внутрішні AML-процедури або створити ризик для безпеки.

14. Зберігання даних і записів

Компанія зберігає дані та записи, пов’язані з AML/KYC, транзакціями, P2P-угодами, перевірками, спорами, обмеженнями та звітністю, протягом строку, передбаченого застосовним законодавством, вимогами партнерів, внутрішніми правилами управління ризиками та Політикою конфіденційності.

До таких даних можуть належати:

- KYC-дані;
- документи користувача;
- результати перевірок;
- санкційні та PEP-збіги;
- профіль ризику;
- історія операцій;
- блокчейн-адреси;
- txid/hash транзакцій;
- дані P2P-угод;
- підтвердження оплати;
- матеріали спорів;
- листування з підтримкою;
- внутрішні рішення щодо обмежень;
- записи про запити компетентних органів.

Видалення акаунта, відкликання згоди або припинення використання Платформи не завжди означає негайне видалення AML/KYC-даних, якщо їх зберігання вимагається або допускається законом, правилами AML/KYC/CTF, захистом прав Компанії, вирішенням спорів або виконанням запитів компетентних органів.

15. Треті особи та постачальники послуг

Компанія може залучати третіх осіб для виконання AML/KYC-процедур, включно з:

- постачальниками перевірки документів;
- постачальниками liveness-перевірки;
- постачальниками санкційного скринінгу;
- постачальниками PEP/adverse media-перевірки;
- постачальниками блокчейн-аналітики;
- платіжними партнерами;
- банками, процесингами та обмінними провайдерами;
- юридичними, комплаєнс- та аудиторськими консультантами;
- постачальниками інфраструктури та безпеки.

Провайдери можуть бути зазначені категоріями без конкретних назв, якщо інше не вимагається законом, договором із провайдером або окремою політикою Компанії.

Компанія може перевіряти партнерів і постачальників на предмет санкцій, репутації, ліцензій, дозволів, ризиків і здатності дотримуватися вимог безпеки та конфіденційності.

16. Обов’язки користувача

Користувач зобов’язується:

- не використовувати Платформу для забороненої діяльності;
- надавати достовірні відомості;
- своєчасно відповідати на запити Компанії;
- надавати документи та пояснення, якщо вони запитані;
- використовувати лише законно належні йому кошти;
- не використовувати чужі банківські картки, рахунки, гаманці або реквізити без законної підстави;
- не надавати підроблені документи, чеки, скриншоти або квитанції;
- не обходити ліміти, перевірки, санкційні обмеження або правила Платформи;
- не створювати кілька акаунтів для обходу обмежень;
- дотримуватися застосовного законодавства;
- самостійно оцінювати законність своїх операцій у країні проживання.

Відмова від співпраці, ухилення від перевірки, надання неправдивих відомостей або спроба обійти AML/KYC-контроль може призвести до обмеження або припинення обслуговування.

17. Конфіденційність AML/KYC-процедур

Користувач розуміє, що Компанія не розкриває:

- точні критерії ризику;
- внутрішні red flags;
- пороги моніторингу;
- алгоритми скорингу;
- джерела AML-даних;
- деталі розслідування;
- причини подання звіту компетентним органам;
- деталі внутрішніх рішень;
- інформацію, розкриття якої може порушити закон, безпеку або ефективність AML/KYC-контролю.

18. Зміна Політики

Компанія має право змінювати цю Політику в будь-який час. Актуальна версія публікується на сайті https://kashbi.io або в інтерфейсі Платформи.

Продовження використання Платформи після публікації оновленої версії означає згоду користувача з новою редакцією Політики, якщо інше не передбачено

застосовним законодавством.

19. Мовні версії

Ця Політика може бути опублікована російською, казахською, англійською та іншими мовами.

Якщо застосовне законодавство вимагає пріоритету певної мовної версії, застосовується така версія. В інших випадках у разі розбіжностей між мовними версіями пріоритет має російська версія.

20. Контакти

З питань цієї Політики користувач може звернутися:

- Компанія: F-Tech
- Країна реєстрації: Kazakhstan
- Сайт: https://kashbi.io
- Застосунок: KashBi
- Email: legal@kashbi.io
- Telegram: kashbi_support
- Юридична адреса: 44/1 Al-Farabi Avenue, Apartment 207