

AML/KYCポリシー

本AML/KYCポリシー（以下「本ポリシー」といいます）は、Kazakhstanで登録されたF-Tech（以下「当社」といいます）が、ウェブサイト<https://kashbi.io>、アプリケーションKashBi、Telegramボット、Telegram Mini App、Web版、API、暗号資産・法定通貨ウォレット、P2Pプラットフォーム、および当社のその他関連サービス（総称して「プラットフォーム」といいます）の利用に関連して、マネー・ローンダリング、テロ資金供与、制裁回避、詐欺、その他違法または禁止された活動を防止するための方針を定めるものです。

本ポリシーは利用規約の一部を構成し、プライバシーポリシー、P2P取引規則、手数料規則、リスク警告、および当社のその他文書とあわせて適用されます。

ユーザーは、プラットフォームを利用し、アカウントを作成し、残高に入金し、デジタル資産を出金し、P2P取引を作成または承諾し、確認手続きを受け、またはその他の方法でプラットフォームとやり取りすることにより、本ポリシーを読み、その条項を遵守することに同意したものとみなされます。

ユーザーが本ポリシーに同意しない場合、プラットフォームの利用を停止しなければなりません。

1. 目的および適用範囲

1.1. 本ポリシーの目的

本ポリシーの目的は、以下を目的とする主要な原則、規則および措置を定めることです。

- プラットフォームがマネー・ローンダリングに利用されることを防止すること。
- テロ資金供与を防止すること。
- 制裁回避を防止すること。
- 詐欺、スキャンム、フィッシングおよびその他違法行為を防止すること。
- 高リスクのユーザー、操作、アドレスおよび法域を特定し評価すること。
- デジタル資産に関する操作およびP2P取引を監視すること。
- 適用法令、パートナー、AML/KYCサービス提供者、銀行、決済事業者および管轄当局の要求事項を遵守すること。
- ユーザー、当社、プラットフォームおよび当社の事業上の信用を保護すること。

1.2. 適用範囲

本ポリシーは、以下の利用者を含む、プラットフォームのすべてのユーザーに適用されます。

- 暗号資産・法定通貨ウォレット。
- P2Pプラットフォーム。

- Telegram Mini App。
- Telegramボット。
- Web版。
- デジタル資産の入金および出金機能。
- 内部送金。
- 当該機能が利用可能な場合のP2P外の法定通貨取引。
- サポートサービスおよび紛争解決。

1.3. リスクベース・アプローチ

当社はリスクベース・アプローチを採用します。これは、KYC、AMLチェック、限度額、書類提出要求、強化デュー・ディリジェンス、監視、制限その他の措置が、ユーザー、操作、法域、決済方法、デジタル資産、ブロックチェーンアドレス、ユーザーの行動その他の要素のリスク水準に応じて適用されることを意味します。

プラットフォームはprivacy-firstを重視するものとして位置付けられています。当社は、個人データの収集を最小限に抑え、必要がない限り本人確認書類を求めないよう努めます。ただし、privacy-firstは完全な匿名性を意味するものではなく、法令、プラットフォーム規則、パートナーの要求事項または本ポリシーにより要求または許容される場合には、データ処理、ユーザー確認、取引審査、操作制限、または管轄当局への情報提供を排除するものではありません。

2. 用語および定義

2.1. AML

AMLとは、違法な出所を有する資金に関連する操作の検出、防止、調査および制限を含む、マネー・ローンダリング対策を意味します。

2.2. KYC

KYCとは、「Know Your Customer」すなわち顧客確認手続を意味し、リスク、限度額、操作、適用法令またはパートナーの要求事項を考慮して必要となる場合に、ユーザーの識別、確認および評価を含みます。

2.3. CDD

CDDとは、顧客デュー・ディリジェンスを意味し、ユーザー、その活動、資金源、操作目的およびリスクプロファイルに関する情報の収集および分析を含みます。

2.4. EDD

EDDとは、高リスクのユーザー、操作または状況に適用される強化デュー・ディリジェンスを意味します。EDDには、追加書類の要求、資金源の確認、取引の拡張分析、公開情報の確認、制裁およびPEPチェック、ならびに当社責任者レベルでの継続的なサービス提供の承認が含まれる場合があります。

2.5. KYT

KYTとは、「Know Your Transaction」すなわち取引確認手続を意味し、操作、ブロックチェーンアドレス、資金源、ユーザーの行動、関連ウォレット、P2Pパターンおよび特定の操作に関連するその他のデータの分析を含みます。

2.6. PEP

PEPとは、政治的に重要な地位にある者、その家族および当該者と密接な関係を有する者を意味し、これらの者が腐敗、制裁、評判その他のリスクの観点から強化された注意を要する場合を含みます。

2.7. 制裁

制裁とは、国家、国際機関、管轄当局により課される、または当社のパートナーを通じて適用される、経済的、金融的、貿易上、人的、地域的その他の制限措置を意味します。

2.8. 禁止法域

禁止法域とは、法令、制裁、高いAMLリスク、パートナーの要求事項、社内リスク管理規則その他の事情により、当社がサービス提供を制限または禁止する国、地域または区域を意味します。

禁止法域の一覧は、本ポリシーに必ずしも掲載されるものではなく、プラットフォームのインターフェース、当社の内部規則、パートナー文書または個別通知により定められる場合があります。

2.9. 疑わしい活動

疑わしい活動とは、マネー・ローンダリング、テロ資金供与、制裁回避、詐欺、スキャン、第三者データの使用、複数アカウントの使用、違法行為またはその他受け入れられないリスクを示唆し得る、操作、行動、資金源、P2P取引、アドレス、決済方法、アカウントその他の要素を意味します。

2.10. Red flags / 警告兆候

Red flagsとは、リスクの上昇または追加審査の必要性を示す可能性のある兆候または指標を意味します。

3. AML/KYC管理体制

3.1. 責任者

当社は、AML/KYC手続の実施、リスク管理、取引監視、疑わしい活動の審査、管轄当局との連携および内部規則の維持を担当する責任者またはチームを任命することができます。

3.2. 内部規則

当社は、内部規則、指示、リスク基準、red flags、確認手続、限度額、監視シナリオおよび意思決定規則を策定し適用します。

これらの内部文書は当社の機密情報であり、その開示が管理の有効性、プラットフォームの安全性、法令遵守、第三者の権利または調査上の利益を損なう可能性がある場合、ユーザーに開示されません。

3.3. 手続の更新

当社は、以下を考慮してAML/KYC手続を更新することができます。

- 法令の変更。
- 新しい製品および機能。
- 新しい詐欺スキーム。
- FATF勧告およびその他国際基準。
- パートナーの要求事項。
- 内部レビューの結果。
- セキュリティインシデント。
- 制裁体制の変更。
- マネー・ローンダリングおよびテロ資金供与の新たな類型。

4. リスク評価

4.1. 一般的リスク評価

当社は、プラットフォーム、ユーザー、製品、デジタル資産、法域、アクセスチャネル、P2P取引、決済方法、P2P外の法定通貨取引、ブロックチェーンネットワークおよびサービス提供者に関連するAML/KYCリスクについて、定期的な評価を実施することがあります。

4.2. リスク要素

リスク評価において、当社は以下を考慮することがあります。

- ユーザーの居住国、国籍、所在地またはIPベースの地理情報。
- アカountの種類および登録方法。
- 操作履歴。
- 操作金額および頻度。
- 使用されるデジタル資産およびネットワーク。
- 送信者および受信者のブロックチェーンアドレス。
- アドレスとミキサー、ダークネット市場、ハッキング、ランサムウェア、スキャンプロジェクト、制裁対象アドレスまたはその他高リスクの資金源との関連。
- P2P取引の利用。
- 選択された法定通貨の決済方法。
- 紛争における行動。
- 他のユーザーからの苦情。
- 複数アカウントの使用または過去にブロックされたアカウントとの関連。
- VPN、プロキシその他所在地を隠す手段の使用。

- 情報提供の拒否。
- データの不一致。
- PEPステータス。
- 制裁リストとの一致。
- adverse mediaその他の評判上の要素。
- パートナーおよび管轄当局の要求事項。

4.3. リスク区分

当社は、ユーザー、操作、アドレスまたは取引に対して、低、中、高または受け入れられないリスクなどの内部リスク区分を付与することができます。

リスク区分は以下に影響する場合があります。

- 利用可能な機能。
- 限度額。
- KYCの必要性。
- EDDの必要性。
- 操作処理速度。
- 出金可否。
- P2Pへのアクセス。
- 手動審査の必要性。
- 凍結またはサービス拒否の可能性。

当社は、内部リスク区分、算定方法、正確な基準またはスコアリング結果をユーザーに開示する義務を負いません。

5. KYC/CDD：ユーザー確認

5.1. 一般的方針

当社は、法令、インターフェース、パートナーの要求事項または特定機能により別段定められる場合を除き、すべてのユーザーに対して一律に完全なKYC確認を求めるものではありません。確認はリスクベースで適用されます。

5.2. KYCが必要となる場合

当社は、以下の場合にKYCまたは追加情報を求めることがあります。

- 限度額に達した場合。
- 大口操作。
- 通常と異なる操作。
- 疑わしい活動。

- 紛争の開始。
- 出金要求。
- アドレスまたは取引に関するAML一致。
- 高リスク法域との関連。
- P2P外の法定通貨機能の利用。
- 決済パートナー、銀行、交換サービス提供者またはAML/KYC提供者の要求。
- 管轄当局からの要求。
- アカウントアクセスの回復。
- 複数アカウント、詐欺または第三者データ利用の疑い。
- 確認を要するその他の事情。

5.3. 要求される可能性のあるデータ

リスク水準に応じて、当社は以下を要求する場合があります。

- 氏名、父称またはその他の完全な氏名。
- 生年月日。
- 国籍。
- 居住国。
- 居住住所。
- メールアドレス。
- 電話番号。
- 本人確認書類。
- 写真、自撮り、ビデオ確認またはライブネスチェック。
- 住所確認書類。
- 資金源の証明。
- 資産源泉の証明。
- 操作目的の確認。
- 明細書、領収書、支払証明または支払確認。
- P2P取引に関する書類。
- PEPとの関連に関する情報。
- リスク評価に必要なその他の書類または説明。

5.4. データの確認

当社は、提供されたデータを以下の方法で確認することがあります。

- 手動。
- 自動化システム。

- 外部AML/KYC提供者。
- 制裁リストおよびPEPリスト。
- 公開情報。
- ブロックチェーン分析。
- パートナー、ユーザー、銀行、決済事業者または管轄当局から受領した情報。

5.5. ユーザーの協力義務

ユーザーは、要求された情報および書類を適時、正確かつ完全に提供しなければなりません。

ユーザーがデータの提供を拒否し、虚偽または矛盾する情報を提供し、要求に応答せず、または確認を回避しようとした場合、当社は機能制限、操作停止、資産凍結、取引取消、サービス拒否またはアカウント閉鎖を行うことがあります。

5.6. 再確認

当社は、ユーザーが過去に確認を通過している場合であっても、以下の場合には書類または情報を再度要求することができます。

- ユーザーのデータが変更された場合。
- 本人確認書類の有効期限が満了した場合。
- ユーザーの活動が変化した場合。
- 新たなリスクが発生した場合。
- ユーザーが新たな限度額に達した場合。
- 新機能が利用可能になった場合。
- 法令またはパートナーの要求事項が変更された場合。
- 紛争または疑わしい活動が発生した場合。

6. 強化デュー・ディリジェンス（EDD）

6.1. EDDが適用される場合

当社は、ユーザー、操作、アドレス、P2P取引、法域または行動が高いリスクを有する場合、EDDを適用することがあります。

EDDは、特に以下の場合に適用されることがあります。

- ユーザーがPEPである、またはPEPと関連している場合。
- ユーザーが高リスク法域と関連している場合。
- 操作が大口、複雑、異常または経済的に説明困難である場合。
- 資金が高リスクのブロックチェーンアドレスから到着した場合。
- 操作がミキサー、ダークネット市場、ハッキング、ランサムウェア、スキャンム、制裁対象アドレスまたはその他red flagsに関連する場合。

- ユーザーが頻繁に紛争を開始し、または紛争で不利な結果となる場合。
- 複数アカウント使用の兆候がある場合。
- 第三者の決済情報またはアカウントを使用している兆候がある場合。
- ユーザーが資金源を説明できない場合。
- ユーザーの回答に矛盾がある場合。
- パートナーまたは管轄当局の要求により確認が必要な場合。

6.2. EDD措置

EDDには以下が含まれる場合があります。

- 追加書類の要求。
- 資金源の確認。
- 資産源泉の確認。
- 操作目的の確認。
- 公開情報の確認。
- adverse mediaの確認。
- ブロックチェーン履歴の詳細分析。
- 限度額の引き下げ。
- 資金の一時凍結。
- 操作の手動承認。
- 操作の拒否。
- サービスの終了。

6.3. EDDの結果

EDDの結果、当社は以下を行うことがあります。

- 操作を許可すること。
- 限度または条件付きで操作を許可すること。
- 追加情報を要求すること。
- 操作を拒否すること。
- 許容され可能な場合に資金を返還すること。
- 資金を凍結すること。
- アカウントを制限すること。
- アカウントを閉鎖すること。
- 法令により要求または許容される場合に管轄当局へ情報を提供すること。

7. KYTおよび取引監視

7.1. 一般的監視

当社は、以下を含むユーザーの操作について、継続的または選択的な監視を行うことがあります。

- デジタル資産の入金。
- デジタル資産の出金。
- 内部送金。
- P2P取引。
- 当該機能が利用可能な場合のP2P外の法定通貨取引。
- 操作の試行。
- 取消済み操作。
- 紛争または苦情に関連する操作。

7.2. ブロックチェーン分析

当社は、アドレス、取引、アドレスクラスター、資金源および関連主体のリスクを評価するために、ブロックチェーン分析を使用することがあります。

審査では、以下との関連を考慮する場合があります。

- 制裁対象アドレス。
- ダークネット市場。
- ミキサーおよび難読化サービス。
- ランサムウェア。
- ハッキングおよび盗難資金。
- スキャンプロジェクト。
- 詐欺スキーム。
- 違法サービス。
- 高リスクの取引所または交換業者。
- その他リスクが高い資金源。

7.3. P2P監視

P2P取引において、当社は以下を分析することがあります。

- 取引頻度。
- 取引金額。
- 当事者の行動。
- 取消回数。

- 紛争回数。
- 苦情。
- 支払証明。
- 決済情報の一致。
- アカウント間の関連。
- 複数アカウント使用の兆候。
- 決済データの不一致。
- プラットフォーム規則外へ取引を移そうとする試み。
- 第三者の銀行口座、カードまたは決済情報の使用。

7.4. 限度および遅延

当社は、特定のユーザー、操作、取引、アドレス、資産、決済方法または法域に対し、限度、遅延、手動審査または追加要件を設定することがあります。

操作は審査完了まで遅延または停止される場合があります。

8. Red flags：疑わしい活動の兆候

Red flagsには、特に以下が含まれる場合があります。

- ユーザーがデータまたは書類の提供を拒否すること。
- 偽造、改ざんまたは矛盾する書類の提供。
- 第三者のデータ、カード、口座またはウォレットの使用。
- 複数アカウントを使用しようとする事。
- P2P取引の頻繁な取消。
- P2P取引に関する頻繁な紛争。
- 偽造された領収書、支払証明または支払スクリーンショット。
- 支払人名とユーザー名の不一致。
- 明らかな経済目的のない迅速な入金および出金。
- 操作を複数の小口金額に分割すること。
- ユーザーの通常の行動と一致しない操作。
- 高リスクのブロックチェーンアドレスの使用。
- ミキサー、ダークネット市場、ハッキング、ランサムウェア、スキャンまたは制裁対象アドレスとの関連。
- 取扱高の急激な増加。
- 限度回避の試み。
- 制限回避のためのVPN、プロキシその他所在地を隠す手段の使用。

- 取引相手またはサポートに対する攻撃的な圧力。
- 資金源の説明拒否。
- 取引をプラットフォーム外に移そうとする試み。
- 他のユーザーからの苦情。
- 公開情報における否定的情報。
- 制裁、PEPまたはadverse mediaソースとの一致。

1つのred flagの存在が常に違反を意味するものではありませんが、追加審査、操作制限その他措置の根拠となる場合があります。

9. 制裁および禁止関係

当社は、法令、制裁、パートナーの要求事項または内部リスク管理規則により禁止される場合、ユーザーとの関係を開始または継続しません。

当社は、ユーザーが以下に該当する場合、サービス拒否、アカウント制限、資産凍結または関係終了を行うことがあります。

- 制裁リストに掲載されている場合。
- 制裁リスト掲載者と関連している場合。
- 禁止法域に所在する場合。
- 禁止対象者の利益のために行動している場合。
- 制裁回避のためにプラットフォームを利用している場合。
- 制裁チェックに必要な情報の提供を拒否する場合。

当社は、登録時、操作前、操作後、制裁リスト変更時、紛争開始時、資金出金時またはその他の場合に制裁チェックを行うことがあります。

10. 禁止活動

ユーザーは、以下の目的でプラットフォームを使用してはなりません。

- マネー・ロンダリング。
- テロ資金供与。
- 制裁回避。
- 詐欺、スキーム、フィッシングまたはソーシャルエンジニアリング。
- 盗難資金、アカウント、カード、書類または個人データの取引。
- 法的根拠なく第三者の銀行カード、口座、ウォレットまたは決済情報を使用すること。
- 麻薬、武器、危険物質またはその他禁止物品の違法取引。
- 違法賭博。

- 違法金融サービス。
- ダークネット活動。
- 過激派、テロリストまたは禁止活動への資金提供。
- 第三者の権利侵害。
- 偽造書類、領収書、支払証明またはスクリーンショットの使用。
- 複数アカウント使用および制限回避。
- 当社が違法、高リスクまたは受け入れられないと判断するその他の活動。

11. リスク検出時の当社措置

当社が疑わしい活動、AML/KYCリスク、制裁リスク、本ポリシー違反またはユーザーによる協力拒否を検出した場合、当社は以下を行うことがあります。

- 追加情報を要求すること。
- KYCまたはEDDを要求すること。
- 限度額を引き下げること。
- 操作を遅延させること。
- 操作を拒否すること。
- P2P取引を取り消すこと。
- P2P機能を制限すること。
- 資産を凍結または留保すること。
- 出金を制限すること。
- アカウントを一時的にブロックすること。
- アカウントを閉鎖すること。
- 可能であり、許容され、かつ法令で禁止されない場合に送信者へ資金を返還すること。
- プラットフォーム規則に定められる場合、適用手数料、ネットワーク費用または返還費用を控除すること。
- 法令により要求または許容される場合に管轄当局へ情報を提供すること。
- プラットフォーム、ユーザー、パートナーおよび当社を保護するためのその他合理的措置を講じること。

当社は、通知が法令、AML/KYC/CTF要件、制裁規則、調査上の利益、プラットフォームの安全性または第三者の権利に反するおそれがある場合、これらの措置について事前にユーザーへ通知する義務を負いません。

12. AML/KYC拒否時の資金返還

AML/KYC審査の結果、操作が拒否され、またはサービスが制限された場合、当社は、可能かつ許容される場合、デジタル資産を元の送信者アドレスまたは当社がリスクおよび法的観点から許容可能と判断する別のアドレスへ返還することがあります。

以下の場合、返還が不可能または遅延することがあります。

- 資金が制裁対象アドレスと関連している場合。
- 資金が犯罪活動と関連している場合。
- 管轄当局から要求を受けている場合。
- 返還が法令に違反するおそれがある場合。
- 元のアドレスが利用不能、高リスクまたは技術的に不適切である場合。
- 追加審査が必要な場合。
- 資金がすでに留保、凍結され、または紛争に関連している場合。

返還額から、利用規約、手数料ページ<https://kashbi.io/information/fees>、プラットフォームのインターフェースまたは別途の規則に定められている場合、ネットワーク手数料、サービス手数料、処理費用その他適用費用が控除されることがあります。

当該返還に係る手数料または費用の具体的な金額は本ポリシーには定められておらず、当該費用が適用される場合、手数料ページ<https://kashbi.io/information/fees>、プラットフォームのインターフェースまたは別途の規則により定められることがあります。

13. 報告および当局との連携

当社は、法令により要求または許容される場合、管轄当局、金融インテリジェンス機関、法執行機関、裁判所、規制当局、銀行、決済事業者その他権限ある者と連携することがあります。

当社は、以下の場合に、ユーザー、アカウント、取引、P2P取引、紛争、アドレス、決済データその他の事情に関する情報を提供することがあります。

- 適法な要求を受けた場合。
- 疑わしい活動を報告する義務がある場合。
- 制裁要件を遵守する必要がある場合。
- 当社、ユーザーまたは第三者の権利を保護する必要がある場合。
- 詐欺、マネー・ローンダリングまたはテロ資金供与を防止する必要がある場合。

当社は、通知が法令により禁止され、調査を妨げ、内部AML手続を明らかにし、またはセキュリティリスクを生じさせるおそれがある場合、当該提供についてユーザーへ通知する義務を負いません。

14. データおよび記録の保存

当社は、AML/KYC、取引、P2P取引、審査、紛争、制限および報告に関連するデータおよび記録を、適用法令、パートナーの要求事項、内部リスク管理規則およびプライバシーポリシーに定められる期間保存します。

これらのデータには以下が含まれる場合があります。

- KYCデータ。
- ユーザー書類。
- 確認結果。
- 制裁およびPEPとの一致。
- リスクプロファイル。
- 操作履歴。
- ブロックチェーンアドレス。
- 取引txid/hash。
- P2P取引データ。
- 支払証明。
- 紛争資料。
- サポートとの通信。
- 制限に関する内部決定。
- 管轄当局からの要求記録。

アカウントの削除、同意の撤回またはプラットフォーム利用の終了は、法令、AML/KYC/CTF規則、当社の権利保護、紛争解決または管轄当局からの要求への対応のために保存が要求または許容される場合、AML/KYCデータの即時削除を常に意味するものではありません。

15. 第三者およびサービス提供者

当社は、AML/KYC手続を実施するために、以下を含む第三者を利用することがあります。

- 書類確認提供者。
- ライブネスチェック提供者。
- 制裁スクリーニング提供者。
- PEP/adverse mediaスクリーニング提供者。
- ブロックチェーン分析提供者。
- 決済パートナー。
- 銀行、処理業者および交換サービス提供者。
- 法務、コンプライアンスおよび監査アドバイザー。

- ・ インフラおよびセキュリティ提供者。

提供者は、法令、提供者との契約または当社の別途ポリシーにより別段要求される場合を除き、具体的名称ではなくカテゴリーで表示される場合があります。

当社は、パートナーおよび提供者について、制裁、評判、ライセンス、許認可、リスクならびにセキュリティおよび機密保持要件を遵守する能力を確認することがあります。

16. ユーザーの義務

ユーザーは以下を約束します。

- ・ 禁止活動のためにプラットフォームを利用しないこと。
- ・ 正確な情報を提供すること。
- ・ 当社の要求に適時対応すること。
- ・ 要求された場合に書類および説明を提供すること。
- ・ 合法的に自己に帰属する資金のみを使用すること。
- ・ 法的根拠なく第三者の銀行カード、口座、ウォレットまたは決済情報を使用しないこと。
- ・ 偽造書類、領収書、スクリーンショットまたは支払証明を提供しないこと。
- ・ 限度、チェック、制裁制限またはプラットフォーム規則を回避しないこと。
- ・ 制限回避のために複数アカウントを作成しないこと。
- ・ 適用法令を遵守すること。
- ・ 居住国における自己の操作の合法性を自ら評価すること。

協力拒否、確認回避、虚偽情報の提供またはAML/KYC管理の回避の試みは、サービス制限または終了につながる場合があります。

17. AML/KYC手続の機密性

ユーザーは、当社が以下を開示しないことを理解します。

- ・ 正確なリスク基準。
- ・ 内部red flags。
- ・ 監視しきい値。
- ・ スコアリングアルゴリズム。
- ・ AMLデータの出所。
- ・ 調査の詳細。
- ・ 管轄当局への報告提出理由。
- ・ 内部決定の詳細。
- ・ 開示により法令、セキュリティまたはAML/KYC管理の有効性を損なうおそれのある情報。

18. 本ポリシーの変更

当社はいつでも本ポリシーを変更することができます。最新版はウェブサイト<https://kashbi.io>またはプラットフォームのインターフェースに掲載されます。

更新版の掲載後もプラットフォームの利用を継続することは、適用法令に別段の定めがない限り、ユーザーが本ポリシーの新しい版に同意したことを意味します。

19. 言語版

本ポリシーは、ロシア語、カザフ語、英語その他の言語で公表される場合があります。

適用法令が特定の言語版の優先を要求する場合、当該言語版が適用されます。それ以外の場合、言語版間に相違があるときは、ロシア語版が優先します。

20. 連絡先

本ポリシーに関する質問について、ユーザーは以下に連絡することができます。

- 会社: F-Tech
- 登録国: Kazakhstan
- ウェブサイト: <https://kashbi.io>
- アプリケーション: KashBi
- Email: legal@kashbi.io
- Telegram: [kashbi_support](https://t.me/kashbi_support)
- 法的住所: 44/1 Al-Farabi Avenue, Apartment 207