Politique AML/KYC

La présente Politique AML/KYC (la « Politique ») décrit l'approche de F-Tech, enregistrée au Kazakhstan (la « Société », « nous », « notre », « nos »), en matière de prévention du blanchiment de capitaux, du financement du terrorisme, du contournement des sanctions, de la fraude et des autres activités illégales ou interdites lors de l'utilisation du site web https://kashbi.io, de l'application KashBi, du bot Telegram, de la Telegram Mini App, de la version web, de l'API, du portefeuille crypto-fiat, de la plateforme P2P et des autres services associés de la Société, désignés collectivement par la « Plateforme ».

La présente Politique fait partie des Conditions d'utilisation et s'applique conjointement avec la Politique de confidentialité, les règles relatives aux transactions P2P, les règles tarifaires, les avertissements sur les risques et les autres documents de la Société.

En utilisant la Plateforme, en créant un compte, en approvisionnant un solde, en retirant des actifs numériques, en créant ou en acceptant une transaction P2P, en effectuant une vérification ou en interagissant de toute autre manière avec la Plateforme, l'utilisateur confirme qu'il a pris connaissance de la présente Politique et accepte d'en respecter les dispositions.

Si l'utilisateur n'accepte pas la présente Politique, il doit cesser d'utiliser la Plateforme.

1. Objet et champ d'application

1.1. Objet de la Politique

La présente Politique a pour objet d'établir les principes, règles et mesures essentiels visant à :

- empêcher l'utilisation de la Plateforme à des fins de blanchiment de capitaux ;
- empêcher le financement du terrorisme ;
- empêcher le contournement des sanctions ;
- empêcher la fraude, les escroqueries, l'hameçonnage et les autres activités illicites ;
- identifier et évaluer les utilisateurs, opérations, adresses et juridictions à haut risque ;
- surveiller les opérations portant sur des actifs numériques ainsi que les transactions P2P ;
- respecter les exigences légales applicables, les exigences des partenaires, des prestataires de services AML/KYC, des banques, des prestataires de paiement et des autorités compétentes ;
- protéger les utilisateurs, la Société, la Plateforme et la réputation commerciale de la Société.

1.2. Champ d'application

La présente Politique s'applique à tous les utilisateurs de la Plateforme, y compris aux utilisateurs :

- du portefeuille crypto-fiat ;

- de la plateforme P2P ;
- de la Telegram Mini App ;
- du bot Telegram ;
- de la version web ;
- des fonctions de dépôt et de retrait d'actifs numériques ;
- des transferts internes ;
- des opérations en monnaie fiat hors P2P, lorsque ces fonctions sont disponibles ;
- des services de support et de règlement des litiges.

1.3. Approche fondée sur les risques

La Société applique une approche fondée sur les risques. Cela signifie que le KYC, les contrôles AML, les limites, les demandes de documents, la vigilance renforcée, la surveillance, les restrictions et les autres mesures sont appliqués proportionnellement au niveau de risque de l'utilisateur, de l'opération, de la juridiction, du moyen de paiement, de l'actif numérique, de l'adresse blockchain, du comportement de l'utilisateur et d'autres facteurs.

La Plateforme se positionne comme privacy-first : la Société cherche à réduire au minimum la collecte de données à caractère personnel et à ne pas demander de pièces d'identité sans nécessité. En même temps, privacy-first ne signifie pas un anonymat complet et n'exclut ni le traitement des données, ni la vérification des utilisateurs, ni le filtrage des opérations, ni la restriction des transactions, ni la communication d'informations aux autorités compétentes lorsque cela est requis ou permis par la loi, les règles de la Plateforme, les exigences des partenaires ou la présente Politique.

2. Termes et définitions

2.1. AML

L'AML désigne les mesures de lutte contre le blanchiment de capitaux, y compris la détection, la prévention, l'investigation et la restriction des opérations liées à des fonds d'origine illicite.

2.2. KYC

Le KYC désigne la procédure de « connaissance du client », comprenant l'identification, la vérification et l'évaluation d'un utilisateur lorsque cette procédure est requise compte tenu du risque, des limites, d'une opération, du droit applicable ou des exigences des partenaires.

2.3. CDD

Le CDD désigne la vigilance à l'égard de la clientèle, comprenant la collecte et l'analyse d'informations sur l'utilisateur, son activité, l'origine de ses fonds, la finalité de ses opérations et son profil de risque.

2.4. EDD

L'EDD désigne la vigilance renforcée appliquée aux utilisateurs, opérations ou situations présentant un risque élevé. L'EDD peut inclure des demandes de documents supplémentaires, la confirmation de l'origine des fonds, une analyse approfondie des opérations, des vérifications en sources ouvertes, un filtrage des sanctions et des PPE,

ainsi que l'approbation de la poursuite de la relation au niveau des personnes responsables de la Société.

2.5. KYT

Le KYT désigne la procédure de « connaissance de la transaction », comprenant l'analyse des opérations, des adresses blockchain, des origines de fonds, du comportement des utilisateurs, des portefeuilles associés, des schémas P2P et d'autres données relatives à une opération donnée.

2.6. PPE

Une PPE désigne une personne politiquement exposée, ainsi que les membres de sa famille et les personnes qui lui sont étroitement associées, lorsque ces personnes requièrent une attention renforcée du point de vue des risques de corruption, de sanctions, de réputation ou d'autres risques.

2.7. Sanctions

Les sanctions désignent les mesures restrictives économiques, financières, commerciales, individuelles, territoriales ou autres, imposées par des États, des organisations internationales, des autorités compétentes, ou applicables par l'intermédiaire des partenaires de la Société.

2.8. Juridiction interdite

Une juridiction interdite désigne un pays, un territoire ou une région pour lesquels la Société limite ou interdit ses services en raison de la loi, de sanctions, d'un risque AML élevé, des exigences de partenaires, de règles internes de gestion des risques ou d'autres circonstances.

La liste des juridictions interdites n'est pas nécessairement publiée dans la présente Politique et peut être déterminée dans l'interface de la Plateforme, dans les règles internes de la Société, dans les documents des partenaires ou dans des avis distincts.

2.9. Activité suspecte

Une activité suspecte désigne une opération, un comportement, une origine de fonds, une transaction P2P, une adresse, un moyen de paiement, un compte ou tout autre facteur pouvant indiquer un blanchiment de capitaux, un financement du terrorisme, un contournement des sanctions, une fraude, une escroquerie, l'utilisation des données d'autrui, du multicompte, une activité illicite ou tout autre risque inacceptable.

2.10. Signaux d'alerte

Les signaux d'alerte (red flags) désignent des signes ou indicateurs pouvant révéler un risque élevé ou la nécessité d'un examen complémentaire.

3. Organisation des contrôles AML/KYC

3.1. Personnes responsables

La Société peut désigner une personne ou une équipe responsable de la mise en œuvre des procédures AML/KYC, de la gestion des risques, de la surveillance des opérations, de l'examen des activités suspectes, des échanges avec les autorités compétentes et de la tenue des règles internes.

3.2. Règles internes

La Société élabore et applique des règles internes, des instructions, des critères de risque, des signaux d'alerte, des procédures de vérification, des limites, des scénarios de surveillance et des règles de prise de décision.

Ces documents internes constituent des informations confidentielles de la Société et ne sont pas communiqués aux utilisateurs si cette communication est susceptible de nuire à l'efficacité des contrôles, à la sécurité de la Plateforme, au respect de la loi, aux droits de tiers ou aux intérêts d'une enquête.

3.3. Mise à jour des procédures

La Société peut mettre à jour ses procédures AML/KYC en tenant compte :

- des évolutions législatives ;
- des nouveaux produits et fonctionnalités ;
- des nouveaux schémas de fraude ;
- des recommandations du GAFI et des autres normes internationales ;
- des exigences des partenaires ;
- des résultats des contrôles internes ;
- des incidents de sécurité ;
- des évolutions des régimes de sanctions ;
- des nouvelles typologies de blanchiment de capitaux et de financement du terrorisme.

4. Évaluation des risques

4.1. Évaluation générale des risques

La Société peut procéder à une évaluation régulière des risques AML/KYC liés à la Plateforme, aux utilisateurs, aux produits, aux actifs numériques, aux juridictions, aux canaux d'accès, aux transactions P2P, aux moyens de paiement, aux opérations en monnaie fiat hors P2P, aux réseaux blockchain et aux prestataires de services.

4.2. Facteurs de risque

Lors de l'évaluation des risques, la Société peut prendre en compte :

- le pays de résidence, la nationalité, la localisation de l'utilisateur ou sa géolocalisation déterminée par l'adresse IP ;
- le type de compte et le mode d'inscription ;
- l'historique des opérations ;
- les montants et la fréquence des opérations ;
- les actifs numériques et les réseaux utilisés ;
- les adresses blockchain des expéditeurs et des destinataires ;
- les liens entre des adresses et des mixeurs, des places de marché du darknet, des piratages, des rançongiciels, des projets frauduleux, des adresses sanctionnées ou d'autres sources à haut risque ;
- le recours aux transactions P2P ;
- les moyens de paiement fiat sélectionnés ;

- le comportement lors des litiges ;
- les plaintes d'autres utilisateurs ;
- le multicompte ou les liens avec des comptes précédemment bloqués ;
- l'utilisation de VPN, de proxys ou d'autres moyens de dissimuler la localisation ;
- le refus de fournir des informations ;
- l'incohérence des données ;
- le statut de PPE ;
- les correspondances avec des listes de sanctions ;
- la presse défavorable et d'autres facteurs de réputation ;
- les exigences des partenaires et des autorités compétentes.

4.3. Catégories de risque

La Société peut attribuer des catégories de risque internes aux utilisateurs, aux opérations, aux adresses ou aux transactions, telles que risque faible, moyen, élevé ou inacceptable.

La catégorie de risque peut influer sur :

- les fonctions disponibles ;
- les limites ;
- la nécessité d'un KYC ;
- la nécessité d'un EDD ;
- la rapidité de traitement des opérations ;
- la disponibilité des retraits ;
- l'accès au P2P ;
- la nécessité d'un examen manuel ;
- la probabilité d'un gel des fonds ou d'un refus de service.

La Société n'est pas tenue de communiquer à l'utilisateur la catégorie de risque interne, la méthodologie de calcul, les critères exacts ou les résultats du scoring.

5. KYC/CDD : vérification des utilisateurs

5.1. Approche générale

La Société n'exige pas par défaut une vérification KYC complète de tous les utilisateurs, sauf disposition contraire de la loi, de l'interface, des exigences des partenaires ou d'une fonction particulière. La vérification est appliquée selon une approche fondée sur les risques.

5.2. Cas dans lesquels le KYC peut être exigé

La Société peut demander un KYC ou des informations complémentaires dans les cas suivants :

- atteinte des limites ;
- opération d'un montant important ;
- opération inhabituelle ;

- activité suspecte ;
- ouverture d'un litige ;
- demande de retrait ;
- correspondance AML concernant une adresse ou une opération ;
- lien avec une juridiction à haut risque ;
- utilisation d'une fonction fiat hors P2P ;
- exigence d'un partenaire de paiement, d'une banque, d'un prestataire de change ou d'un prestataire AML/KYC ;
- demande d'une autorité compétente ;
- récupération de l'accès à un compte ;
- soupçon de multicompte, de fraude ou d'utilisation des données d'autrui ;
- autres circonstances nécessitant une vérification.

5.3. Données pouvant être demandées

Selon le niveau de risque, la Société peut demander :

- le prénom, le nom, le patronyme ou tout autre nom complet ;
- la date de naissance ;
- la nationalité ;
- le pays de résidence ;
- l'adresse du domicile ;
- l'e-mail ;
- le numéro de téléphone ;
- une pièce d'identité ;
- une photographie, un selfie, une vérification vidéo ou un contrôle de vivacité ;
- un justificatif de domicile ;
- un justificatif de l'origine des fonds ;
- un justificatif de l'origine du patrimoine ;
- une confirmation de la finalité d'une opération ;
- un relevé, un reçu, un ordre de paiement ou une preuve de paiement ;
- des documents relatifs à une transaction P2P ;
- des informations sur un lien avec une PPE ;
- tout autre document ou explication nécessaire à l'évaluation des risques.

5.4. Vérification des données

La Société peut vérifier les données fournies :

- manuellement ;
- au moyen de systèmes automatisés ;
- par l'intermédiaire de prestataires AML/KYC externes ;
- au moyen de listes de sanctions et de PPE ;
- au moyen de sources ouvertes ;

- au moyen d'analyses blockchain ;
- au moyen d'informations reçues de partenaires, d'utilisateurs, de banques, de prestataires de paiement ou d'autorités compétentes.

5.5. Obligation de coopération de l'utilisateur

L'utilisateur doit fournir les informations et documents demandés de manière rapide, exacte et complète.

Si l'utilisateur refuse de fournir des données, communique des informations fausses ou incohérentes, ne répond pas aux demandes ou tente de contourner la vérification, la Société peut restreindre des fonctions, suspendre des opérations, geler des actifs, annuler des transactions, refuser le service ou clôturer le compte.

5.6. Nouvelle vérification

La Société peut demander à nouveau des documents ou des informations, même si l'utilisateur a déjà été vérifié, lorsque :

- les données de l'utilisateur ont changé ;
- la pièce d'identité est arrivée à expiration ;
- l'activité de l'utilisateur a changé ;
- de nouveaux risques sont apparus ;
- l'utilisateur a atteint de nouvelles limites ;
- une nouvelle fonction est devenue disponible ;
- les exigences légales ou celles des partenaires ont changé ;
- un litige ou une activité suspecte est survenu.

6. Vigilance renforcée (EDD)

6.1. Cas d'application de l'EDD

La Société peut appliquer l'EDD lorsqu'un utilisateur, une opération, une adresse, une transaction P2P, une juridiction ou un comportement présente un risque élevé.

L'EDD peut s'appliquer, en particulier, lorsque :

- l'utilisateur est une PPE ou est lié à une PPE ;
- l'utilisateur est lié à une juridiction à haut risque ;
- l'opération est d'un montant important, complexe, inhabituelle ou économiquement inexplicable ;
- les fonds proviennent d'une adresse blockchain à haut risque ;
- l'opération est associée à des mixeurs, des places de marché du darknet, des piratages, des rançongiciels, des escroqueries, des adresses sanctionnées ou d'autres signaux d'alerte ;
- l'utilisateur ouvre ou perd fréquemment des litiges ;
- des indices de multicompte sont présents ;
- des indices d'utilisation des coordonnées de paiement ou du compte d'un tiers sont présents ;
- l'utilisateur ne peut pas expliquer l'origine des fonds ;

- l'utilisateur donne des réponses incohérentes ;
- une confirmation est requise à la demande d'un partenaire ou d'une autorité compétente.

6.2. Mesures d'EDD

L'EDD peut comprendre :

- des demandes de documents supplémentaires ;
- la confirmation de l'origine des fonds ;
- la confirmation de l'origine du patrimoine ;
- la confirmation de la finalité d'une opération ;
- des vérifications en sources ouvertes ;
- des vérifications de presse défavorable ;
- une analyse approfondie de l'historique blockchain ;
- une réduction des limites ;
- un gel temporaire des fonds ;
- une validation manuelle d'une opération ;
- le refus d'une opération ;
- la fin de la relation de service.

6.3. Issues de l'EDD

À l'issue de l'EDD, la Société peut :

- autoriser l'opération ;
- autoriser l'opération sous conditions ou avec des limites ;
- demander des informations complémentaires ;
- refuser l'opération ;
- restituer les fonds, lorsque cela est permis et possible ;
- geler les fonds ;
- restreindre le compte ;
- clôturer le compte ;
- communiquer des informations aux autorités compétentes lorsque la loi l'exige ou le permet.

7. KYT et surveillance des opérations

7.1. Surveillance générale

La Société peut assurer une surveillance continue ou sélective des opérations des utilisateurs, notamment :

- les dépôts d'actifs numériques ;
- les retraits d'actifs numériques ;
- les transferts internes ;
- les transactions P2P ;

- les opérations en monnaie fiat hors P2P, lorsque ces fonctions sont disponibles ;
- les tentatives d'opérations ;
- les opérations annulées ;
- les opérations liées à des litiges ou à des plaintes.

7.2. Analyse blockchain

La Société peut recourir à l'analyse blockchain pour évaluer le risque des adresses, des transactions, des groupes d'adresses, des origines de fonds et des entités associées.

L'examen peut tenir compte des liens avec :

- des adresses sanctionnées ;
- des places de marché du darknet ;
- des mixeurs et services d'obscurcissement ;
- des rançongiciels ;
- des piratages et des fonds volés ;
- des projets frauduleux ;
- des montages frauduleux ;
- des services illégaux ;
- des plateformes ou bureaux d'échange à haut risque ;
- d'autres sources de risque élevé.

7.3. Surveillance du P2P

Dans les transactions P2P, la Société peut analyser :

- la fréquence des transactions ;
- les montants des transactions ;
- le comportement des parties ;
- le nombre d'annulations ;
- le nombre de litiges ;
- les plaintes ;
- les preuves de paiement ;
- la concordance des coordonnées de paiement ;
- les liens entre comptes ;
- les indices de multicompte ;
- les incohérences dans les données de paiement ;
- les tentatives de sortir une transaction du cadre des règles de la Plateforme ;
- l'utilisation de comptes bancaires, de cartes ou de coordonnées de paiement de tiers.

7.4. Limites et délais

La Société peut fixer des limites, des délais, des examens manuels ou des exigences supplémentaires pour certains utilisateurs, opérations, transactions, adresses, actifs, moyens de paiement ou juridictions.

Une opération peut être retardée ou suspendue jusqu'à la fin de l'examen.

8. Signaux d'alerte : indices d'activité suspecte

Les signaux d'alerte peuvent notamment inclure :

- le refus de l'utilisateur de fournir des données ou des documents ;
- la fourniture de documents falsifiés, modifiés ou incohérents ;
- l'utilisation des données, cartes, comptes ou portefeuilles d'autrui ;
- une tentative d'utiliser plusieurs comptes ;
- l'annulation fréquente de transactions P2P ;
- des litiges fréquents dans les transactions P2P ;
- des reçus, ordres de paiement ou captures d'écran de paiement falsifiés ;
- une discordance entre le nom du payeur et celui de l'utilisateur ;
- le dépôt et le retrait rapides de fonds sans finalité économique apparente ;
- le fractionnement des opérations en plusieurs montants plus faibles ;
- des opérations incompatibles avec le comportement habituel de l'utilisateur ;
- l'utilisation d'adresses blockchain à haut risque ;
- des liens avec des mixeurs, des places de marché du darknet, des piratages, des rançongiciels, des escroqueries ou des adresses sanctionnées ;
- une forte augmentation du volume d'activité ;
- des tentatives de contourner les limites ;
- l'utilisation de VPN, de proxys ou d'autres moyens de dissimuler la localisation afin de contourner des restrictions ;
- une pression agressive exercée sur une contrepartie ou sur le support ;
- le refus d'expliquer l'origine des fonds ;
- une tentative de sortir une transaction de la Plateforme ;
- des plaintes d'autres utilisateurs ;
- des informations négatives issues de sources ouvertes ;
- des correspondances avec des sources relatives aux sanctions, aux PPE ou à la presse défavorable.

La présence d'un seul signal d'alerte ne signifie pas toujours qu'il y a infraction, mais elle peut justifier un examen complémentaire, la restriction d'une opération ou d'autres mesures.

9. Sanctions et relations interdites

La Société n'établit ni ne poursuit de relations avec des utilisateurs lorsque cela est interdit par la loi, par des sanctions, par les exigences de partenaires ou par des règles internes de gestion des risques.

La Société peut refuser le service, restreindre un compte, geler des actifs ou mettre fin à la relation si l'utilisateur :

- figure sur une liste de sanctions ;
- est lié à une personne figurant sur une liste de sanctions ;

- se trouve dans une juridiction interdite ;
- agit dans l'intérêt d'une personne visée par une interdiction ;
- utilise la Plateforme pour contourner des sanctions ;
- refuse de fournir les informations nécessaires au filtrage des sanctions.

La Société peut procéder au filtrage des sanctions lors de l'inscription, avant une opération, après une opération, lors de la mise à jour des listes de sanctions, lors de l'ouverture d'un litige, lors d'un retrait de fonds ou dans d'autres cas.

10. Activités interdites

Il est interdit à l'utilisateur d'utiliser la Plateforme aux fins de :

- blanchiment de capitaux ;
- financement du terrorisme ;
- contournement de sanctions ;
- fraude, escroquerie, hameçonnage ou ingénierie sociale ;
- commerce de fonds, de comptes, de cartes, de documents ou de données personnelles volés ;
- utilisation de cartes bancaires, comptes, portefeuilles ou coordonnées de paiement d'autrui sans fondement légal ;
- trafic illégal de stupéfiants, d'armes, de substances dangereuses ou d'autres biens interdits ;
- jeux d'argent illégaux ;
- services financiers illégaux ;
- activités sur le darknet ;
- financement d'activités extrémistes, terroristes ou autrement interdites ;
- atteinte aux droits de tiers ;
- utilisation de documents, reçus, ordres de paiement ou captures d'écran falsifiés ;
- multicompte et contournement de restrictions ;
- toute autre activité que la Société considère comme illégale, à haut risque ou inacceptable.

11. Mesures prises par la Société en cas de détection d'un risque

Si la Société détecte une activité suspecte, un risque AML/KYC, un risque de sanctions, une violation de la présente Politique ou un refus de coopérer de la part de l'utilisateur, elle peut :

- demander des informations complémentaires ;
- exiger un KYC ou un EDD ;
- réduire les limites ;
- retarder une opération ;
- refuser une opération ;

- annuler une transaction P2P ;
- restreindre les fonctions P2P ;
- geler ou réserver des actifs ;
- restreindre les retraits ;
- bloquer temporairement le compte ;
- clôturer le compte ;
- restituer les fonds à l'expéditeur, lorsque cela est possible, permis et non interdit par la loi ;
- retenir les frais applicables, les coûts de réseau ou les coûts de traitement du remboursement lorsque les règles de la Plateforme le prévoient ;
- communiquer des informations aux autorités compétentes lorsque la loi l'exige ou le permet ;
- prendre toute autre mesure raisonnable pour protéger la Plateforme, les utilisateurs, les partenaires et la Société.

La Société n'est pas tenue d'informer l'utilisateur au préalable de ces mesures si cette information est susceptible d'enfreindre la loi, les exigences AML/KYC/CTF, les règles relatives aux sanctions, les intérêts d'une enquête, la sécurité de la Plateforme ou les droits de tiers.

12. Restitution des fonds en cas de refus AML/KYC

Si une opération est rejetée ou si le service est restreint à la suite d'un examen AML/KYC, la Société peut, lorsque cela est possible et permis, restituer les actifs numériques à l'adresse de l'expéditeur d'origine ou à une autre adresse qu'elle juge acceptable du point de vue des risques et du droit.

Une restitution peut être impossible ou retardée lorsque :

- les fonds sont liés à une adresse sanctionnée ;
- les fonds sont liés à une activité criminelle ;
- une demande d'une autorité compétente a été reçue ;
- la restitution est susceptible d'enfreindre la loi ;
- l'adresse d'origine est indisponible, à haut risque ou techniquement inadaptée ;
- un examen complémentaire est nécessaire ;
- les fonds sont déjà réservés, gelés ou liés à un litige.

Les frais de réseau, les frais de service, les coûts de traitement et les autres coûts applicables peuvent être retenus sur le montant restitué lorsque les Conditions d'utilisation, la page des frais https://kashbi.io/information/fees, l'interface de la Plateforme ou des règles distinctes le prévoient.

Le montant exact de tout frais ou commission appliqué à une telle restitution n'est pas fixé dans la présente Politique et peut être déterminé par la page des frais https://kashbi.io/information/fees, l'interface de la Plateforme ou des règles distinctes, si de tels frais s'appliquent.

13. Déclarations et relations avec les autorités

La Société peut coopérer avec les autorités compétentes, les cellules de renseignement financier, les autorités répressives, les tribunaux, les régulateurs, les banques, les prestataires de paiement et d'autres personnes habilitées lorsque la loi l'exige ou le permet.

La Société peut communiquer des informations sur un utilisateur, un compte, une opération, une transaction P2P, un litige, une adresse, des données de paiement ou d'autres circonstances lorsque :

- une demande licite a été reçue ;
- il existe une obligation de déclarer une activité suspecte ;
- des exigences en matière de sanctions doivent être respectées ;
- cela est nécessaire pour protéger les droits de la Société, des utilisateurs ou de tiers ;
- cela est nécessaire pour prévenir la fraude, le blanchiment de capitaux ou le financement du terrorisme.

La Société n'est pas tenue d'informer l'utilisateur d'une telle communication si cette information est interdite par la loi, est susceptible d'entraver une enquête, de révéler des procédures AML internes ou de créer un risque de sécurité.

14. Conservation des données et des enregistrements

La Société conserve les données et enregistrements relatifs à l'AML/KYC, aux opérations, aux transactions P2P, aux examens, aux litiges, aux restrictions et aux déclarations pendant la durée prévue par le droit applicable, les exigences des partenaires, les règles internes de gestion des risques et la Politique de confidentialité.

Ces données peuvent comprendre :

- les données KYC ;
- les documents des utilisateurs ;
- les résultats des vérifications ;
- les correspondances avec les listes de sanctions et de PPE ;
- le profil de risque ;
- l'historique des opérations ;
- les adresses blockchain ;
- les txid/hachages des transactions ;
- les données des transactions P2P ;
- les preuves de paiement ;
- les pièces des litiges ;
- la correspondance avec le support ;
- les décisions internes de restriction ;
- les enregistrements des demandes des autorités compétentes.

La suppression d'un compte, le retrait du consentement ou la fin de l'utilisation de la

Plateforme ne signifient pas toujours la suppression immédiate des données AML/KYC lorsque leur conservation est exigée ou permise par la loi, par les règles AML/KYC/CTF, par la protection des droits de la Société, par le règlement des litiges ou par le traitement des demandes des autorités compétentes.

15. Tiers et prestataires de services

La Société peut faire appel à des tiers pour l'exécution des procédures AML/KYC, notamment :

- des prestataires de vérification de documents ;
- des prestataires de contrôle de vivacité ;
- des prestataires de filtrage des sanctions ;
- des prestataires de filtrage PPE/presse défavorable ;
- des prestataires d'analyse blockchain ;
- des partenaires de paiement ;
- des banques, processeurs et prestataires de change ;
- des conseils juridiques, en conformité et en audit ;
- des fournisseurs d'infrastructure et de sécurité.

Les prestataires peuvent être décrits par catégorie, sans mention de leurs noms, sauf si la loi, un accord avec un prestataire ou une politique distincte de la Société l'exige.

La Société peut évaluer ses partenaires et prestataires au regard des sanctions, de la réputation, des licences, des autorisations, des risques et de leur capacité à respecter les exigences de sécurité et de confidentialité.

16. Obligations de l'utilisateur

L'utilisateur s'engage à :

- ne pas utiliser la Plateforme pour des activités interdites ;
- fournir des informations exactes ;
- répondre aux demandes de la Société dans les délais ;
- fournir les documents et explications demandés ;
- n'utiliser que des fonds lui appartenant légalement ;
- ne pas utiliser les cartes bancaires, comptes, portefeuilles ou coordonnées de paiement d'autrui sans fondement légal ;
- ne pas fournir de documents, reçus, captures d'écran ou ordres de paiement falsifiés ;
- ne pas contourner les limites, les contrôles, les restrictions liées aux sanctions ou les règles de la Plateforme ;
- ne pas créer plusieurs comptes afin de contourner des restrictions ;
- respecter le droit applicable ;
- évaluer lui-même la légalité de ses opérations dans son pays de résidence.

Le refus de coopérer, le contournement de la vérification, la communication d'informations fausses ou une tentative de contourner les contrôles AML/KYC peuvent entraîner la

restriction ou la fin du service.

17. Confidentialité des procédures AML/KYC

L'utilisateur comprend que la Société ne communique pas :

- les critères de risque exacts ;
- les signaux d'alerte internes ;
- les seuils de surveillance ;
- les algorithmes de scoring ;
- les sources des données AML ;
- les détails des enquêtes ;
- les motifs d'une déclaration adressée aux autorités compétentes ;
- les détails des décisions internes ;
- les informations dont la divulgation pourrait enfreindre la loi, la sécurité ou l'efficacité des contrôles AML/KYC.

18. Modifications de la Politique

La Société peut modifier la présente Politique à tout moment. La version en vigueur est publiée sur le site web https://kashbi.io ou dans l'interface de la Plateforme.

La poursuite de l'utilisation de la Plateforme après la publication d'une version mise à jour vaut acceptation par l'utilisateur de la nouvelle version de la Politique, sauf disposition contraire du droit applicable.

19. Versions linguistiques

La présente Politique peut être publiée dans d'autres langues.

Si le droit applicable exige qu'une version linguistique particulière prévale, cette version s'applique. Dans tous les autres cas, en cas de divergence entre les versions linguistiques, la version russe prévaut.

20. Contacts

Pour toute question relative à la présente Politique, l'utilisateur peut contacter :

- Société : F-Tech
- Pays d'enregistrement : Kazakhstan
- Site web : https://kashbi.io
- Application : KashBi
- E-mail : legal@kashbi.io
- Telegram : kashbi_support
- Adresse légale : 44/1 Al-Farabi Avenue, Apartment 207