

# Politique de confidentialité

---

La présente Politique de confidentialité (la « Politique ») décrit comment F-Tech (la « Société », « nous », « notre », « nos ») collecte, utilise, conserve, transfère et protège les données à caractère personnel des utilisateurs 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 et des autres services associés de la Société (collectivement, la « Plateforme »).

La présente Politique s'applique aux utilisateurs, aux visiteurs du site web, aux titulaires de comptes enregistrés, aux participants aux transactions P2P, aux titulaires de portefeuilles, aux personnes s'adressant au support et aux autres personnes dont les données peuvent être traitées lors de l'utilisation de la Plateforme.

La présente Politique fait partie des conditions applicables aux utilisateurs, des règles d'utilisation de la Plateforme, des politiques AML/KYC/CTF et des autres documents de la Société, lorsque ces documents s'appliquent. Si vous n'acceptez pas la présente Politique, veuillez cesser d'utiliser la Plateforme.

## 1. Termes et définitions

**1.1. Données à caractère personnel désigne toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement.**

**1.2. Traitement des données à caractère personnel désigne toute opération ou tout ensemble d'opérations effectuées sur des données à caractère personnel, y compris la collecte, l'enregistrement, l'organisation, l'accumulation, la conservation, la précision, la mise à jour, la modification, l'extraction, l'utilisation, le transfert, la mise à disposition, l'anonymisation, le blocage, l'effacement et la destruction.**

**1.3. Utilisateur désigne une personne physique qui visite le site web, s'inscrit sur la Plateforme, utilise un portefeuille, participe à des transactions P2P, contacte le support ou interagit de toute autre manière avec la Plateforme.**

**1.4. Compte désigne un compte utilisateur sur la Plateforme créé via la Telegram Mini App, le bot Telegram, la version web, l'application mobile ou tout autre moyen disponible.**

**1.5. Actifs numériques désigne les crypto-monnaies, les jetons, les stablecoins et les autres unités de compte numériques prises en charge par la Plateforme.**

**1.6. Transaction P2P désigne une transaction entre utilisateurs de la Plateforme, dans le cadre de laquelle les utilisateurs conviennent eux-mêmes des conditions d'échange, de paiement, de transfert d'actifs numériques, de fonds en monnaie fiat, de biens, de services ou d'autres valeurs, lorsque cette fonctionnalité est fournie par la Plateforme.**

**1.7. AML/KYC/CTF désigne les procédures de lutte contre le blanchiment de capitaux, le financement du terrorisme, le contournement des sanctions, la fraude et les autres activités interdites, ainsi que les procédures d'identification, de vérification et d'évaluation des risques liés aux utilisateurs.**

**1.8. Sous-traitant désigne un tiers qui traite des données à caractère personnel pour le compte de la Société, dans l'intérêt de la Société ou aux fins d'assurer le fonctionnement de la Plateforme.**

## **2. À propos de la Société et coordonnées**

F-Tech est le responsable du traitement, l'opérateur ou toute autre personne responsable des données à caractère personnel traitées dans le cadre de l'utilisation de la Plateforme, sauf disposition contraire du droit applicable ou d'un service particulier.

Coordonnées :

- Site web : <https://kashbi.io>
- Application : KashBi
- E-mail du support : [legal@kashbi.io](mailto:legal@kashbi.io)
- Support Telegram : kashbi\_support
- Pays d'enregistrement : Kazakhstan
- Adresse du siège : 44/1 Al-Farabi Avenue, Apartment 207

## **3. Principes généraux du traitement des données à caractère personnel**

Nous nous efforçons de traiter les données à caractère personnel de manière licite, loyale et transparente. Nous suivons les principes de licéité, de limitation des finalités, de minimisation des données, d'exactitude, de limitation de la conservation, de sécurité et de confidentialité.

Nous ne cherchons pas à collecter plus de données que nécessaire au fonctionnement de la Plateforme, au respect de la loi, à la sécurité, à la prévention de la fraude, au règlement des litiges, aux procédures AML/KYC/CTF et à la protection des droits de la Société et des utilisateurs.

## **4. Bases légales du traitement**

Selon la finalité concernée et le droit applicable, nous pouvons traiter les données à caractère personnel sur les bases légales suivantes :

- le consentement de l'utilisateur ;
- l'exécution d'un contrat ou l'exécution de mesures précontractuelles ;
- le respect d'obligations légales ;
- l'intérêt légitime de la Société ;

- la protection des intérêts vitaux de l'utilisateur ou d'autres personnes, le cas échéant.

Lorsque le traitement est fondé sur le consentement, l'utilisateur a le droit de le retirer. Le retrait du consentement n'affecte pas la licéité du traitement effectué avant ce retrait et n'empêche pas le traitement des données sur d'autres bases légales.

## **5. Données que nous pouvons traiter**

### **5.1. Données de compte et d'inscription :**

- identifiant Telegram ;
- nom d'utilisateur Telegram ;
- prénom, nom ou nom affiché provenant de Telegram, s'ils sont transmis par Telegram ;
- avatar ou photo de profil, s'il est disponible via Telegram ou téléchargé par l'utilisateur ;
- initData de la Telegram WebApp, nécessaire à l'autorisation et à la vérification de l'authenticité de la connexion ;
- informations sur la liaison d'un compte Telegram à un compte créé dans la version web ;
- adresse e-mail ;
- numéro de téléphone ;
- identifiant de connexion ;
- mot de passe sous forme de hachage cryptographique pour la version web ;
- code PIN sous forme de hachage cryptographique ou d'une autre valeur technique protégée pour la Telegram Mini App ;
- informations sur l'activation et l'utilisation de la 2FA pour la version web ;
- paramètres biométriques uniquement sous la forme d'une indication technique de l'activation de la fonction, sans réception ni conservation de gabarits biométriques ;
- autres facteurs de sécurité sous forme d'identifiants techniques, de hachages ou d'indications d'activation d'une fonction ;
- date d'inscription, statut du compte, langue de l'interface, paramètres de notification ;
- code de parrainage, identifiant de l'utilisateur parrain ou informations sur un programme d'affiliation, le cas échéant.

### **5.2. Données techniques :**

- adresse IP ;
- localisation approximative déterminée à partir de l'adresse IP ;
- données relatives à l'appareil, au navigateur, au système d'exploitation, à la version de l'application et à la langue ;
- identifiants de session ;
- informations de connexion au compte ;

- journaux de sécurité ;
- données relatives aux erreurs, aux pannes, aux événements de l'application et aux diagnostics ;
- date, heure et durée d'utilisation de la Plateforme ;
- informations sur les actions de l'utilisateur dans l'interface, nécessaires à la sécurité, à l'analyse et à l'amélioration du service.

### 5.3. Données relatives au portefeuille et aux opérations sur actifs numériques :

- identifiants internes de portefeuille et de solde ;
- adresses blockchain publiques ;
- memo, tag, commentaire ou autres identifiants de paiement ;
- txid, hachage de transaction, numéro de bloc, nombre de confirmations, réseau, actif, montant, frais ;
- adresses de l'expéditeur et du destinataire sur la blockchain ;
- historique des dépôts, retraits, transferts, transferts internes, blocages, gels, réservations, remboursements, frais et ajustements ;
- informations sur le statut des transactions ;
- données sur l'origine des actifs numériques entrants, lorsque cela est nécessaire à l'analyse AML ou à la vérification de l'origine des fonds ;
- résultats des contrôles de risque automatisés ou manuels des transactions blockchain, lorsque de tels contrôles sont appliqués.

Les données publiques de la blockchain peuvent être accessibles dans les réseaux blockchain concernés indépendamment de la Société. La Société ne contrôle pas les registres publics de la blockchain et ne peut ni supprimer ni modifier les données déjà inscrites dans un réseau blockchain public.

### 5.4. Données relatives aux transactions P2P :

- identifiant d'une annonce, d'une offre ou d'une transaction ;
- rôle de l'utilisateur dans la transaction ;
- type de transaction ;
- actif numérique, réseau et devise de règlement sélectionnés ;
- montant, prix, taux, marge, limites, frais ;
- statut de la transaction ;
- date et heure de création, d'acceptation, de paiement, de confirmation, d'achèvement, d'annulation ou d'ouverture d'un litige ;
- conditions, commentaires et instructions de la transaction ;
- moyen de paiement ;

- coordonnées de paiement fournies par l'utilisateur pour l'exécution de la transaction ;
- confirmations de paiement, reçus, captures d'écran, justificatifs, messages, pièces jointes et autres preuves ;
- correspondance entre les participants à la transaction, lorsque cette fonctionnalité est fournie ;
- actions des modérateurs ou des arbitres dans un litige ;
- issue du litige et motifs de la décision rendue.

L'utilisateur ne doit pas transmettre, via le chat, les descriptions de transactions, les pièces jointes ou d'autres champs, de données à caractère personnel excessives, de données de tiers, de codes secrets, de mots de passe, de phrases de récupération, de clés privées ou d'autres informations confidentielles non nécessaires à l'exécution de la transaction.

### **5.5. Données relatives aux paiements en monnaie fiat**

Dans le cadre des transactions P2P, les paiements en monnaie fiat sont effectués directement entre les utilisateurs, sauf disposition expresse contraire d'un service distinct de la Plateforme. La Société n'est ni une banque, ni un établissement de paiement, ni une partie au transfert de fonds fiat entre utilisateurs ; toutefois, aux fins de l'accompagnement des transactions P2P, du règlement des litiges, de la prévention de la fraude et du respect des exigences applicables, nous pouvons traiter :

- le moyen de paiement sélectionné ;
- le nom du titulaire du compte ou de l'instrument de paiement, s'il est fourni par l'utilisateur ;
- les données masquées de la carte ou du compte ;
- la banque, le système de paiement ou le prestataire ;
- le pays de l'instrument de paiement ;
- le montant, la devise, la date et le statut du paiement ;
- l'identifiant de paiement attribué par le prestataire, si cet identifiant est fourni par l'utilisateur ;
- les informations relatives à un remboursement, une annulation, une rétrofacturation, un litige ou une opération suspecte.

Nous ne devons ni demander ni conserver les données complètes de cartes bancaires, les codes CVV/CVC, les mots de passe d'applications bancaires, les codes de confirmation de paiement ou d'autres données de paiement secrètes.

### **5.6. Données AML/KYC/CTF et d'évaluation des risques**

Nous appliquons une approche fondée sur les risques en matière d'AML/KYC/CTF. L'identification, la vérification, les contrôles supplémentaires ou les demandes de documents peuvent ne pas s'appliquer par défaut à tous les utilisateurs, mais peuvent être mis en œuvre lorsque cela est nécessaire au regard du droit applicable, des règles internes de gestion des risques, des limites, du type de transaction, d'indices d'activité

suspecte, des exigences des partenaires, d'un litige, d'une demande au support ou d'autres facteurs de risque.

Lorsque des procédures AML/KYC/CTF sont appliquées à un utilisateur, nous pouvons traiter :

- 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 ;
- le numéro de téléphone ;
- l'e-mail ;
- une pièce d'identité ;
- une photographie, un selfie, une vérification vidéo ou un contrôle de vivacité ;
- les informations sur le bénéficiaire effectif, l'origine des fonds, l'origine du patrimoine, la profession ou la finalité des opérations, le cas échéant ;
- les résultats des filtrages relatifs aux sanctions, aux PPE, à la presse défavorable et autres ;
- les résultats des contrôles AML des adresses et des transactions blockchain ;
- le profil de risque interne de l'utilisateur ;
- les documents et explications fournis par l'utilisateur à la demande de la Société ;
- les informations relatives à une activité suspecte, inhabituelle, interdite ou à haut risque.

Le seul fait de s'inscrire sur la Plateforme ne signifie pas que l'utilisateur est tenu, dans tous les cas, de suivre une vérification KYC complète, sauf disposition contraire de l'interface, des conditions d'un service particulier ou des exigences applicables.

#### 5.7. Données du service de support :

- coordonnées ;
- contenu de la demande ;
- pièces jointes, captures d'écran, documents et messages ;
- historique de la correspondance ;
- enregistrements des demandes, si le canal de communication concerné prévoit un enregistrement ;
- informations sur la résolution de la demande ;
- données nécessaires pour confirmer la propriété du compte.

#### 5.8. Données marketing et de communication :

- consentements et désabonnements aux envois ;
- e-mail, nom d'utilisateur Telegram, identifiant Telegram ou autre canal de communication ;
- historique des notifications ;
- préférences relatives à la langue et aux types de messages ;
- statistiques de distribution et d'interaction avec les messages, le cas échéant.

Nous pouvons envoyer des messages de service, d'information et de marketing relatifs à la Plateforme, à la sécurité, aux mises à jour, aux nouvelles fonctionnalités, aux modifications des conditions, aux promotions ou à d'autres offres de la Société. Nous ne cherchons pas à envoyer à l'utilisateur des messages excessifs, trompeurs ou intrusifs. L'utilisateur peut refuser les communications marketing lorsque ce refus est prévu par le droit applicable ou par l'interface de la Plateforme. Les avis de service et les notifications juridiquement significatives peuvent être envoyés indépendamment de tout refus des messages marketing.

## **6. Finalités du traitement des données à caractère personnel**

Nous pouvons traiter les données à caractère personnel aux fins suivantes :

- l'inscription et la gestion du compte ;
- l'autorisation, l'authentification et la récupération de l'accès ;
- la mise à disposition de portefeuilles et la réalisation d'opérations sur actifs numériques ;
- le traitement des dépôts, des retraits, des transferts internes, des soldes, des frais et des confirmations ;
- la fourniture des fonctions P2P, la création d'offres, l'ouverture et l'achèvement des transactions ;
- la réservation, le blocage ou la libération d'actifs numériques ;
- l'échange de messages et de preuves entre les participants à une transaction ;
- le règlement des litiges et l'arbitrage ;
- l'enregistrement des moyens de paiement et la vérification des confirmations de paiement dans les litiges P2P ;
- l'AML/KYC/CTF, le filtrage des sanctions et la gestion des risques ;
- la surveillance des transactions et la vérification des adresses blockchain ;
- la sécurité, la prévention de la fraude, du multicompte, du spam, de l'hameçonnage, des attaques et des autres infractions ;
- l'assistance aux utilisateurs ;
- l'amélioration de la Plateforme, la correction des erreurs, les tests de fonctionnalités et l'analyse ;

- les finalités juridiques, le traitement des réclamations et la protection des droits de la Société.

## **7. Cookies et technologies similaires**

Nous pouvons utiliser le stockage local, le stockage de session, des identifiants techniques de session, des journaux serveur, des outils d'analyse internes non fondés sur les cookies et d'autres technologies similaires à des fins d'autorisation, d'enregistrement des paramètres, de protection des sessions, de prévention de la fraude, d'analyse, de diagnostic des erreurs, d'amélioration du fonctionnement de la Plateforme et de respect des exigences de sécurité.

Si, à l'avenir, la Société commence à utiliser des cookies ou des outils d'analyse tiers fondés sur les cookies, ce traitement sera décrit dans la présente Politique, dans une Politique relative aux cookies distincte ou dans une interface de consentement, lorsque le droit applicable l'exige.

## **8. Traitement automatisé et profilage**

Nous pouvons utiliser des outils automatisés et semi-automatisés pour analyser les événements techniques, les transactions, les risques AML, les activités suspectes, les violations des règles, le multicompte et d'autres facteurs de sécurité.

La Plateforme se positionne comme privacy-first : nous cherchons à réduire au minimum la collecte de données à caractère personnel, à ne pas demander de pièces d'identité sans nécessité et à appliquer une approche des contrôles fondée sur les risques. Privacy-first ne signifie pas un anonymat complet et n'exclut pas le traitement des données nécessaires à la sécurité, au respect de la loi, aux procédures AML/KYC/CTF, au règlement des litiges, à la prévention de la fraude et à la protection de la Plateforme.

Ce traitement peut avoir une incidence sur la disponibilité de certaines fonctions de la Plateforme, sur les limites, sur la nécessité d'une vérification supplémentaire, sur la suspension d'une transaction ou sur le renvoi d'un dossier pour examen manuel.

## **9. Transfert de données à des tiers**

Nous ne vendons pas les données à caractère personnel des utilisateurs et ne les transférons pas à des tiers pour leurs propres finalités marketing sans le consentement de l'utilisateur.

Nous pouvons transférer des données à caractère personnel aux catégories de destinataires suivantes :

1. les fournisseurs d'infrastructure ;
2. les prestataires de services AML/KYC/CTF ;
3. les banques, prestataires de paiement et processeurs, uniquement lorsque ces personnes interviennent dans un service ou une opération donnés ;
4. les fournisseurs d'outils d'analyse et de diagnostic ;
5. les fournisseurs de services de communication ;

6. les conseils juridiques, auditeurs et conseils en conformité ;
7. les sociétés affiliées de la Société ;
8. les autorités compétentes ;
9. la contrepartie à une transaction P2P, uniquement dans la mesure nécessaire à l'exécution de la transaction ;
10. les successeurs potentiels ou effectifs en cas de changements dans la structure de la société.

Dans une transaction P2P ordinaire, le paiement en monnaie fiat est effectué directement entre les utilisateurs, et la Société ne traite pas ce paiement en qualité d'intermédiaire de paiement.

## **10. Transferts transfrontaliers de données**

La Plateforme peut recourir à des infrastructures, des partenaires, des prestataires et des sous-traitants situés dans différents pays. À ce titre, les données à caractère personnel peuvent être transférées, conservées et traitées en dehors du pays de résidence de l'utilisateur ou du pays d'enregistrement de la Société.

Lors de transferts transfrontaliers de données, nous prenons des mesures raisonnables pour assurer un niveau approprié de protection des données à caractère personnel, notamment des obligations contractuelles de confidentialité, des mesures de sécurité techniques et organisationnelles, une évaluation préalable des prestataires et d'autres mécanismes prévus par le droit applicable.

## **11. Conservation des données à caractère personnel**

Nous conservons les données à caractère personnel aussi longtemps que nécessaire aux finalités pour lesquelles elles ont été collectées, ainsi que pour le respect des obligations légales, le règlement des litiges, la prévention de la fraude et la protection des droits de la Société et des utilisateurs.

Durées de conservation indicatives :

1. données de compte — pendant toute la durée d'existence du compte et pendant une période raisonnable après sa fermeture ;
2. données relatives aux opérations, aux soldes, aux dépôts, aux retraits et aux transactions P2P — au moins pendant la durée requise par le droit applicable, les règles AML/CTF, les exigences comptables ou les règles internes de gestion des risques ;
3. données AML/KYC/CTF — pendant la durée prévue par le droit applicable ;
4. données du support — pendant la durée nécessaire au traitement de la demande, au règlement d'un litige, à l'amélioration du service et à la protection des droits de la Société ;
5. journaux techniques et données de sécurité — pendant la durée nécessaire à la sécurité, aux diagnostics, aux enquêtes sur les incidents et à la prévention des abus ;
6. données marketing — jusqu'au retrait du consentement ou au refus des

communications par l'utilisateur, sauf si une conservation plus longue est nécessaire pour attester du consentement ou du refus.

La suppression d'un compte ou le retrait du consentement ne signifie pas toujours la suppression immédiate de toutes les données. Nous pouvons conserver des données lorsque cela est nécessaire au respect de la loi, à l'AML/KYC/CTF, à la comptabilité, à la prévention de la fraude, au règlement des litiges, au respect d'exigences judiciaires ou réglementaires, ou à la protection des droits de la Société.

## **12. Données publiques de la blockchain**

L'utilisateur comprend que les opérations sur actifs numériques peuvent être inscrites dans des réseaux blockchain publics ou partiellement publics. La Société n'est pas l'opérateur de ces réseaux, ne contrôle pas leur fonctionnement et ne peut pas supprimer, masquer, modifier ou restreindre la diffusion d'informations déjà publiées sur la blockchain.

## **13. Confidentialité du compte et responsabilité de l'utilisateur**

L'utilisateur est responsable du maintien de la confidentialité des moyens d'accès à son compte, y compris le mot de passe de la version web, le code PIN de la Telegram Mini App, les codes 2FA, les appareils, l'e-mail, le compte Telegram et les autres moyens d'autorisation.

L'utilisateur ne doit divulguer à des tiers ni son mot de passe, ni son code PIN, ni ses codes à usage unique, ni ses codes 2FA, ni sa phrase de récupération, ni ses clés privées, ni ses codes de secours, ni l'accès à son appareil ou à son compte Telegram, ni aucune autre donnée permettant d'accéder au compte ou aux actifs numériques.

La Société ne demande jamais de phrases de récupération, de clés privées, de données complètes de cartes bancaires, de codes CVV/CVC ni de mots de passe de services tiers.

## **14. Données de tiers**

L'utilisateur ne doit pas communiquer à la Société des données à caractère personnel de tiers sans base légale et sans le consentement de ces personnes, lorsque ce consentement est requis. Si l'utilisateur communique des données de tiers dans le cadre d'une transaction P2P, d'une demande au support, d'un litige, d'un téléversement de documents ou de toute autre interaction avec la Plateforme, il confirme qu'il a le droit de communiquer ces données.

## **15. Droits de l'utilisateur**

Selon le droit applicable, l'utilisateur peut disposer du droit :

- d'accéder à ses données à caractère personnel ;
- d'obtenir une copie de ses données ;
- de rectifier des données inexactes, incomplètes ou obsolètes ;
- d'effacer ses données ;

- de limiter le traitement ;
- de s'opposer au traitement ;
- à la portabilité des données ;
- de retirer son consentement ;
- d'introduire une réclamation auprès d'une autorité de contrôle compétente.

Nous pouvons refuser l'effacement total ou partiel des données lorsque leur conservation est nécessaire au respect de la loi, aux obligations AML/KYC/CTF, à la comptabilité, à la prévention de la fraude, au règlement des litiges, à l'exécution de contrats ou à la protection des droits de la Société.

## **16. Sécurité des données à caractère personnel**

Nous appliquons des mesures techniques et organisationnelles raisonnables pour protéger les données à caractère personnel, notamment le chiffrement des transmissions, le contrôle des accès, la séparation des droits, la journalisation des actions, la surveillance des activités suspectes, les sauvegardes, les procédures de réponse aux incidents et des règles internes de sécurité de l'information.

Malgré les mesures prises, aucune méthode de transmission de données sur Internet ni aucun système de stockage n'est absolument sûr. L'utilisateur doit respecter les mesures de sécurité de son côté.

## **17. Enfants et mineurs**

La Plateforme n'est pas destinée aux personnes n'ayant pas atteint l'âge minimum requis pour utiliser de manière autonome les services concernés dans le pays de résidence de l'utilisateur.

## **18. Liens vers des ressources tierces**

La Plateforme peut contenir des liens vers des sites web, applications, portefeuilles, explorateurs de blockchain, services de paiement, ressources Telegram ou autres services externes de tiers. La Société ne contrôle pas ces ressources tierces et n'est pas responsable de leurs politiques de confidentialité, de leur sécurité, de leur contenu ou de leur traitement des données.

## **19. Modifications de la Politique**

Nous pouvons modifier la présente Politique de temps à autre afin de tenir compte des évolutions de la Plateforme, de la législation, des exigences des partenaires, des technologies, des risques ou des processus internes. La version en vigueur de la Politique est publiée sur le site web <https://kashbi.io> ou dans l'interface de la Plateforme.

## **20. Nous contacter**

Pour toute question relative à la présente Politique, au traitement des données à caractère personnel, à l'exercice des droits des utilisateurs ou pour toute réclamation, l'utilisateur

peut contacter :

- Société : F-Tech
- Pays d'enregistrement : Kazakhstan
- Site web : <https://kashbi.io>
- Application : KashBi
- E-mail : [legal@kashbi.io](mailto:legal@kashbi.io)
- Telegram : [kashbi\\_support](https://t.me/kashbi_support)
- Adresse du siège : 44/1 Al-Farabi Avenue, Apartment 207

## **21. Versions linguistiques**

Le présent document peut être publié en plusieurs 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 en langue anglaise prévaut.