

Política AML/KYC

La presente Política AML/KYC (la “Política”) describe el enfoque de F-Tech, registrada en Kazakhstan (la “Compañía”, “nosotros”, “nos”, “nuestro”), para prevenir el lavado de dinero, la financiación del terrorismo, la evasión de sanciones, el fraude y otras actividades ilegales o prohibidas al utilizar el sitio web <https://kashbi.io>, la aplicación KashBi, el bot de Telegram, Telegram Mini App, la versión web, la API, la billetera cripto-fiat, la plataforma P2P y otros servicios relacionados de la Compañía, denominados conjuntamente la “Plataforma”.

La presente Política forma parte de los Términos de Uso y se aplica junto con la Política de Privacidad, las reglas de transacciones P2P, las reglas de comisiones, las advertencias de riesgo y otros documentos de la Compañía.

Al utilizar la Plataforma, crear una cuenta, depositar fondos en el saldo, retirar activos digitales, crear o aceptar una transacción P2P, someterse a una verificación o interactuar de cualquier otra forma con la Plataforma, el usuario confirma que ha leído esta Política y acepta cumplir sus disposiciones.

Si el usuario no está de acuerdo con la presente Política, deberá dejar de utilizar la Plataforma.

1. Finalidad y ámbito de aplicación

1.1. Finalidad de la Política

La finalidad de la presente Política es establecer los principios, reglas y medidas principales dirigidos a:

- prevenir el uso de la Plataforma para el lavado de dinero;
- prevenir la financiación del terrorismo;
- prevenir la evasión de sanciones;
- prevenir el fraude, las estafas, el phishing y otras actividades ilícitas;
- identificar y evaluar usuarios, operaciones, direcciones y jurisdicciones de alto riesgo;
- monitorear operaciones con activos digitales y transacciones P2P;
- cumplir los requisitos legales aplicables, los requisitos de socios, proveedores de servicios AML/KYC, bancos, proveedores de pago y autoridades competentes;
- proteger a los usuarios, a la Compañía, a la Plataforma y la reputación comercial de la Compañía.

1.2. Ámbito de aplicación

La presente Política se aplica a todos los usuarios de la Plataforma, incluidos los usuarios de:

- la billetera cripto-fiat;
- la plataforma P2P;
- Telegram Mini App;

- el bot de Telegram;
- la versión web;
- las funciones de depósito y retiro de activos digitales;
- las transferencias internas;
- las operaciones fiat fuera de P2P, si dichas funciones están disponibles;
- el servicio de soporte y la resolución de disputas.

1.3. Enfoque basado en el riesgo

La Compañía aplica un enfoque basado en el riesgo. Esto significa que las verificaciones KYC y AML, los límites, las solicitudes de documentos, la diligencia debida reforzada, el monitoreo, las restricciones y otras medidas se aplican de forma proporcional al nivel de riesgo del usuario, de la operación, de la jurisdicción, del método de pago, del activo digital, de la dirección blockchain, del comportamiento del usuario y de otros factores.

La Plataforma se posiciona como privacy-first: la Compañía procura minimizar la recopilación de datos personales y no solicitar documentos de identidad sin necesidad. Al mismo tiempo, privacy-first no significa anonimato total y no excluye el tratamiento de datos, la verificación del usuario, la revisión de transacciones, la restricción de operaciones o la transmisión de información a autoridades competentes cuando ello sea requerido o permitido por la ley, las reglas de la Plataforma, los requisitos de los socios o la presente Política.

2. Términos y definiciones

2.1. AML

AML significa medidas contra el lavado de dinero, incluida la detección, prevención, investigación y restricción de operaciones relacionadas con fondos de origen ilícito.

2.2. KYC

KYC significa el procedimiento “Know Your Customer” o “conoce a tu cliente”, que incluye la identificación, verificación y evaluación de un usuario cuando dicho procedimiento sea requerido teniendo en cuenta el riesgo, los límites, una operación, la legislación aplicable o los requisitos de socios.

2.3. CDD

CDD significa diligencia debida del cliente, incluida la recopilación y el análisis de información sobre el usuario, su actividad, el origen de los fondos, los fines de las operaciones y su perfil de riesgo.

2.4. EDD

EDD significa diligencia debida reforzada aplicada a usuarios, operaciones o situaciones de mayor riesgo. La EDD puede incluir solicitudes de documentos adicionales, confirmación del origen de los fondos, análisis ampliado de transacciones, revisión de fuentes abiertas, verificaciones de sanciones y PEP, así como la aprobación de la continuidad del servicio por parte de las personas responsables de la Compañía.

2.5. KYT

KYT significa el procedimiento “Know Your Transaction” o “conoce tu transacción”, que incluye el análisis de operaciones, direcciones blockchain, fuentes de fondos, comportamiento del usuario, billeteras vinculadas, patrones P2P y otros datos relacionados con una operación específica.

2.6. PEP

PEP significa persona políticamente expuesta, así como sus familiares y personas estrechamente vinculadas a dicha persona, cuando tales personas requieran mayor atención desde la perspectiva de riesgos de corrupción, sanciones, reputación u otros riesgos.

2.7. Sanciones

Sanciones significa medidas restrictivas económicas, financieras, comerciales, personales, territoriales u otras impuestas por Estados, organizaciones internacionales, autoridades competentes o aplicables a través de los socios de la Compañía.

2.8. Jurisdicción prohibida

Jurisdicción prohibida significa un país, territorio o región respecto del cual la Compañía restringe o prohíbe la prestación de servicios por motivos legales, sanciones, alto riesgo AML, requisitos de socios, reglas internas de gestión de riesgos u otras circunstancias.

La lista de jurisdicciones prohibidas no necesariamente se publica en la presente Política y puede determinarse en la interfaz de la Plataforma, en las reglas internas de la Compañía, en documentos de socios o en avisos separados.

2.9. Actividad sospechosa

Actividad sospechosa significa una operación, comportamiento, fuente de fondos, transacción P2P, dirección, método de pago, cuenta u otro factor que pueda indicar lavado de dinero, financiación del terrorismo, evasión de sanciones, fraude, estafa, uso de datos de terceros, uso de múltiples cuentas, actividad ilícita u otro riesgo inaceptable.

2.10. Red flags / señales de alerta

Red flags significa signos o indicadores que pueden señalar un riesgo elevado o la necesidad de una revisión adicional.

3. Organización de los controles AML/KYC

3.1. Personas responsables

La Compañía puede designar a una persona responsable o a un equipo responsable de implementar los procedimientos AML/KYC, gestionar riesgos, monitorear transacciones, revisar actividad sospechosa, interactuar con autoridades competentes y mantener las reglas internas.

3.2. Reglas internas

La Compañía desarrolla y aplica reglas internas, instrucciones, criterios de riesgo, red flags, procedimientos de verificación, límites, escenarios de monitoreo y reglas de toma de decisiones.

Dichos documentos internos constituyen información confidencial de la Compañía y no están sujetos a divulgación a los usuarios si dicha divulgación puede perjudicar la eficacia de los controles, la seguridad de la Plataforma, el cumplimiento de la ley, los derechos de terceros o los intereses de una investigación.

3.3. Actualización de procedimientos

La Compañía puede actualizar los procedimientos AML/KYC teniendo en cuenta:

- cambios en la legislación;
- nuevos productos y funciones;
- nuevos esquemas de fraude;
- recomendaciones del FATF y otros estándares internacionales;
- requisitos de socios;
- resultados de revisiones internas;
- incidentes de seguridad;
- cambios en regímenes de sanciones;
- nuevas tipologías de lavado de dinero y financiación del terrorismo.

4. Evaluación de riesgos

4.1. Evaluación general de riesgos

La Compañía puede realizar evaluaciones periódicas de los riesgos AML/KYC relacionados con la Plataforma, usuarios, productos, activos digitales, jurisdicciones, canales de acceso, transacciones P2P, métodos de pago, operaciones fiat fuera de P2P, redes blockchain y proveedores de servicios.

4.2. Factores de riesgo

Al evaluar el riesgo, la Compañía puede tener en cuenta:

- país de residencia, ciudadanía, ubicación o geolocalización por IP del usuario;
- tipo de cuenta y método de registro;
- historial de operaciones;
- importes y frecuencia de operaciones;
- activos digitales y redes utilizados;
- direcciones blockchain de remitentes y destinatarios;
- vínculos de direcciones con mixers, mercados darknet, hackeos, ransomware, proyectos scam, direcciones sancionadas u otras fuentes de alto riesgo;
- uso de transacciones P2P;
- métodos de pago fiat seleccionados;
- comportamiento en disputas;
- quejas de otros usuarios;
- uso de múltiples cuentas o vínculos con cuentas bloqueadas anteriormente;
- uso de VPN, proxies u otros medios para ocultar la ubicación;
- negativa a proporcionar información;

- inconsistencia de datos;
- condición de PEP;
- coincidencias con sanciones;
- adverse media y otros factores reputacionales;
- requisitos de socios y autoridades competentes.

4.3. Categorías de riesgo

La Compañía puede asignar categorías internas de riesgo a usuarios, operaciones, direcciones o transacciones, por ejemplo, riesgo bajo, medio, alto o inaceptable.

La categoría de riesgo puede afectar:

- las funciones disponibles;
- los límites;
- la necesidad de KYC;
- la necesidad de EDD;
- la velocidad de procesamiento de operaciones;
- la posibilidad de retiro;
- el acceso a P2P;
- la necesidad de revisión manual;
- la probabilidad de congelamiento o negativa de servicio.

La Compañía no está obligada a revelar al usuario la categoría interna de riesgo, la metodología de cálculo, los criterios exactos o los resultados de scoring.

5. KYC/CDD: verificación de usuarios

5.1. Enfoque general

La Compañía no exige verificación KYC completa a todos los usuarios por defecto, salvo que la ley, la interfaz, los requisitos de socios o una función específica dispongan lo contrario. La verificación se aplica sobre una base basada en el riesgo.

5.2. Cuándo puede requerirse KYC

La Compañía puede solicitar KYC o información adicional en los siguientes casos:

- alcanzar límites;
- una operación de gran importe;
- una operación inusual;
- actividad sospechosa;
- apertura de una disputa;
- solicitud de retiro;
- coincidencia AML relacionada con una dirección o transacción;
- vínculo con una jurisdicción de alto riesgo;
- uso de una función fiat fuera de P2P;
- requisito de un socio de pago, banco, proveedor de cambio o proveedor AML/KYC;

- solicitud de una autoridad competente;
- recuperación de acceso a la cuenta;
- sospecha de uso de múltiples cuentas, fraude o uso de datos de terceros;
- otras circunstancias que requieran verificación.

5.3. Qué datos pueden solicitarse

Dependiendo del nivel de riesgo, la Compañía puede solicitar:

- nombre, apellido, segundo nombre o cualquier otro nombre completo;
- fecha de nacimiento;
- ciudadanía;
- país de residencia;
- dirección de residencia;
- email;
- número de teléfono;
- documento de identidad;
- fotografía, selfie, verificación por video o prueba de vida;
- comprobante de domicilio;
- comprobante del origen de los fondos;
- comprobante del origen del patrimonio;
- confirmación del propósito de la operación;
- extracto, recibo, comprobante o confirmación de pago;
- documentos relacionados con una transacción P2P;
- información sobre una conexión con una PEP;
- otros documentos o explicaciones necesarios para evaluar el riesgo.

5.4. Verificación de datos

La Compañía puede verificar los datos proporcionados:

- manualmente;
- mediante sistemas automatizados;
- a través de proveedores externos AML/KYC;
- mediante listas de sanciones y PEP;
- mediante fuentes abiertas;
- mediante analítica blockchain;
- mediante información recibida de socios, usuarios, bancos, proveedores de pago o autoridades competentes.

5.5. Obligación del usuario de cooperar

El usuario debe proporcionar la información y los documentos solicitados de manera oportuna, veraz y completa.

Si el usuario se niega a proporcionar datos, proporciona información falsa o contradictoria, no responde a solicitudes o intenta eludir la verificación, la Compañía puede restringir

funciones, suspender operaciones, congelar activos, cancelar transacciones, denegar el servicio o cerrar la cuenta.

5.6. Reverificación

La Compañía puede solicitar documentos o información nuevamente, incluso si el usuario ya ha pasado una verificación anteriormente, si:

- los datos del usuario han cambiado;
- el documento ha vencido;
- la actividad del usuario ha cambiado;
- han surgido nuevos riesgos;
- el usuario ha alcanzado nuevos límites;
- se ha habilitado una nueva función;
- han cambiado los requisitos legales o de socios;
- ha surgido una disputa o actividad sospechosa.

6. Diligencia debida reforzada EDD

6.1. Cuándo se aplica EDD

La Compañía puede aplicar EDD si un usuario, operación, dirección, transacción P2P, jurisdicción o comportamiento presenta un riesgo elevado.

La EDD puede aplicarse, en particular, si:

- el usuario es una PEP o está relacionado con una PEP;
- el usuario está relacionado con una jurisdicción de alto riesgo;
- la operación es grande, compleja, inusual o económicamente inexplicable;
- los fondos provienen de una dirección blockchain de alto riesgo;
- la operación está relacionada con mixers, mercados darknet, hackeos, ransomware, scam, direcciones sancionadas u otras señales de alerta;
- el usuario abre o pierde disputas con frecuencia;
- existen indicios de uso de múltiples cuentas;
- existen indicios de uso de datos de pago o cuenta de terceros;
- el usuario no puede explicar el origen de los fondos;
- el usuario responde de forma contradictoria a las preguntas;
- se requiere confirmación a solicitud de un socio o autoridad competente.

6.2. Medidas EDD

La EDD puede incluir:

- solicitud de documentos adicionales;
- confirmación del origen de los fondos;
- confirmación del origen del patrimonio;
- confirmación del propósito de la operación;
- revisión de fuentes abiertas;

- revisión de adverse media;
- análisis profundizado del historial blockchain;
- reducción de límites;
- congelamiento temporal de fondos;
- aprobación manual de una operación;
- rechazo de una operación;
- terminación del servicio.

6.3. Resultados de EDD

Como resultado de la EDD, la Compañía puede:

- permitir la operación;
- permitir la operación con límites o condiciones;
- solicitar información adicional;
- rechazar la operación;
- devolver los fondos, si está permitido y es posible;
- congelar los fondos;
- restringir la cuenta;
- cerrar la cuenta;
- transmitir información a autoridades competentes cuando sea requerido o permitido por la ley.

7. KYT y monitoreo de transacciones

7.1. Monitoreo general

La Compañía puede realizar monitoreo continuo o selectivo de las operaciones de los usuarios, incluidas:

- depósitos de activos digitales;
- retiros de activos digitales;
- transferencias internas;
- transacciones P2P;
- operaciones fiat fuera de P2P, si dichas funciones están disponibles;
- intentos de operación;
- operaciones canceladas;
- operaciones relacionadas con disputas o quejas.

7.2. Analítica blockchain

La Compañía puede utilizar analítica blockchain para evaluar el riesgo de direcciones, transacciones, clústeres de direcciones, fuentes de fondos y entidades relacionadas.

La revisión puede tener en cuenta vínculos con:

- direcciones sancionadas;
- mercados darknet;

- mixers y servicios de ofuscación;
- ransomware;
- hackeos y fondos robados;
- proyectos scam;
- esquemas fraudulentos;
- servicios ilegales;
- exchanges o cambiadores de alto riesgo;
- otras fuentes de riesgo elevado.

7.3. Monitoreo P2P

En transacciones P2P, la Compañía puede analizar:

- frecuencia de las transacciones;
- importes de las transacciones;
- comportamiento de las partes;
- número de cancelaciones;
- número de disputas;
- quejas;
- comprobantes de pago;
- coincidencias de datos de pago;
- vínculos entre cuentas;
- indicios de uso de múltiples cuentas;
- inconsistencias en los datos de pago;
- intentos de sacar una transacción fuera de las reglas de la Plataforma;
- uso de cuentas bancarias, tarjetas o datos de pago de terceros.

7.4. Límites y demoras

La Compañía puede establecer límites, demoras, revisiones manuales o requisitos adicionales para determinados usuarios, operaciones, transacciones, direcciones, activos, métodos de pago o jurisdicciones.

Una operación puede demorarse o suspenderse hasta que finalice la revisión.

8. Red flags: indicios de actividad sospechosa

Las red flags pueden incluir, entre otras:

- negativa del usuario a proporcionar datos o documentos;
- presentación de documentos falsificados, alterados o contradictorios;
- uso de datos, tarjetas, cuentas o billeteras de terceros;
- intento de utilizar varias cuentas;
- cancelaciones frecuentes de transacciones P2P;
- disputas frecuentes en transacciones P2P;
- recibos, comprobantes o capturas de pantalla de pago falsificados;

- discrepancia entre el nombre del pagador y el usuario;
- entrada y salida rápida de fondos sin un propósito económico evidente;
- estructuración de operaciones en varios importes pequeños;
- operaciones que no se corresponden con el comportamiento habitual del usuario;
- uso de direcciones blockchain de alto riesgo;
- vínculos con mixers, mercados darknet, hackeos, ransomware, scams o direcciones sancionadas;
- aumento brusco del volumen de operaciones;
- intentos de eludir límites;
- uso de VPN, proxies u otros medios para ocultar la ubicación con el fin de eludir restricciones;
- presión agresiva sobre la contraparte o el soporte;
- negativa a explicar el origen de los fondos;
- intento de sacar una transacción fuera de la Plataforma;
- quejas de otros usuarios;
- información negativa de fuentes abiertas;
- coincidencias con fuentes de sanciones, PEP o adverse media.

La presencia de una sola red flag no siempre significa una infracción, pero puede servir como base para una revisión adicional, restricción de una operación u otras medidas.

9. Sanciones y relaciones prohibidas

La Compañía no establece ni mantiene relaciones con usuarios cuando ello esté prohibido por la ley, sanciones, requisitos de socios o reglas internas de gestión de riesgos.

La Compañía puede denegar el servicio, restringir una cuenta, congelar activos o terminar la relación si el usuario:

- está incluido en una lista de sanciones;
- está relacionado con una persona incluida en una lista de sanciones;
- se encuentra en una jurisdicción prohibida;
- actúa en interés de una persona prohibida;
- utiliza la Plataforma para evadir sanciones;
- se niega a proporcionar información necesaria para la revisión de sanciones.

La Compañía puede realizar revisiones de sanciones durante el registro, antes de una operación, después de una operación, cuando cambien las listas de sanciones, al abrirse una disputa, al retirar fondos o en otros casos.

10. Actividad prohibida

El usuario tiene prohibido utilizar la Plataforma para:

- lavado de dinero;
- financiación del terrorismo;

- evasión de sanciones;
- fraude, scams, phishing o ingeniería social;
- comercio de fondos, cuentas, tarjetas, documentos o datos personales robados;
- uso de tarjetas bancarias, cuentas, billeteras o datos de pago de terceros sin base legal;
- tráfico ilegal de drogas, armas, sustancias peligrosas u otros bienes prohibidos;
- juegos de azar ilegales;
- servicios financieros ilegales;
- actividad en darknet;
- financiación de actividades extremistas, terroristas u otras actividades prohibidas;
- infracción de derechos de terceros;
- uso de documentos, recibos, comprobantes o capturas de pantalla falsificados;
- uso de múltiples cuentas y elusión de restricciones;
- cualquier otra actividad que la Compañía considere ilegal, de alto riesgo o inaceptable.

11. Medidas de la Compañía al detectar un riesgo

Si la Compañía detecta actividad sospechosa, riesgo AML/KYC, riesgo de sanciones, infracción de esta Política o negativa del usuario a cooperar, la Compañía puede:

- solicitar información adicional;
- solicitar KYC o EDD;
- reducir límites;
- demorar una operación;
- rechazar una operación;
- cancelar una transacción P2P;
- restringir funciones P2P;
- congelar o reservar activos;
- restringir retiros;
- bloquear temporalmente la cuenta;
- cerrar la cuenta;
- devolver fondos al remitente, si es posible, está permitido y no está prohibido por la ley;
- retener comisiones aplicables, costos de red o costos de devolución si ello está previsto por las reglas de la Plataforma;
- transmitir información a autoridades competentes cuando sea requerido o permitido por la ley;
- adoptar otras medidas razonables para proteger la Plataforma, los usuarios, los socios y la Compañía.

La Compañía no está obligada a notificar previamente al usuario sobre la aplicación de dichas medidas si la notificación puede infringir la ley, los requisitos AML/KYC/CTF, las reglas de sanciones, los intereses de una investigación, la seguridad de la Plataforma o los derechos de terceros.

12. Devolución de fondos en caso de rechazo AML/KYC

Si una operación es rechazada o el servicio es restringido como resultado de una revisión AML/KYC, la Compañía puede, si es posible y permitido, devolver los activos digitales a la dirección original del remitente o a otra dirección que la Compañía considere aceptable desde una perspectiva de riesgo y legal.

La devolución puede ser imposible o demorarse si:

- los fondos están vinculados a una dirección sancionada;
- los fondos están vinculados a actividad delictiva;
- se ha recibido una solicitud de una autoridad competente;
- la devolución puede infringir la ley;
- la dirección original no está disponible, es de alto riesgo o técnicamente no es apta;
- se requiere una revisión adicional;
- los fondos ya están reservados, congelados o relacionados con una disputa.

Del importe de la devolución pueden retenerse comisiones de red, comisiones de servicio, costos de procesamiento y otros costos aplicables, si están previstos en los Términos de Uso, en la página de comisiones <https://kashbi.io/information/fees>, en la interfaz de la Plataforma o en reglas separadas.

El importe concreto de la comisión o cargo por dicha devolución no se fija en esta Política y puede determinarse en la página de comisiones <https://kashbi.io/information/fees>, en la interfaz de la Plataforma o en reglas separadas, si dicho cargo se aplica.

13. Reportes e interacción con autoridades

La Compañía puede interactuar con autoridades competentes, unidades de inteligencia financiera, autoridades policiales, tribunales, reguladores, bancos, proveedores de pago y otras personas autorizadas cuando sea requerido o permitido por la ley.

La Compañía puede transmitir información sobre un usuario, cuenta, transacción, transacción P2P, disputa, dirección, datos de pago u otras circunstancias si:

- se ha recibido una solicitud legal;
- existe la obligación de reportar actividad sospechosa;
- es necesario cumplir requisitos de sanciones;
- es necesario proteger los derechos de la Compañía, de los usuarios o de terceros;
- es necesario prevenir fraude, lavado de dinero o financiación del terrorismo.

La Compañía no está obligada a notificar al usuario sobre dicha transmisión si la notificación está prohibida por la ley, puede obstaculizar una investigación, revelar procedimientos internos AML o crear un riesgo de seguridad.

14. Conservación de datos y registros

La Compañía conserva datos y registros relacionados con AML/KYC, transacciones, transacciones P2P, revisiones, disputas, restricciones y reportes durante el período previsto por la legislación aplicable, los requisitos de socios, las reglas internas de gestión

de riesgos y la Política de Privacidad.

Dichos datos pueden incluir:

- datos KYC;
- documentos del usuario;
- resultados de verificaciones;
- coincidencias de sanciones y PEP;
- perfil de riesgo;
- historial de operaciones;
- direcciones blockchain;
- txid/hash de transacciones;
- datos de transacciones P2P;
- comprobantes de pago;
- materiales de disputas;
- correspondencia con soporte;
- decisiones internas sobre restricciones;
- registros de solicitudes de autoridades competentes.

La eliminación de una cuenta, la retirada del consentimiento o la terminación del uso de la Plataforma no siempre implica la eliminación inmediata de los datos AML/KYC si su conservación es requerida o permitida por la ley, las reglas AML/KYC/CTF, la protección de los derechos de la Compañía, la resolución de disputas o el cumplimiento de solicitudes de autoridades competentes.

15. Terceros y proveedores de servicios

La Compañía puede contratar a terceros para realizar procedimientos AML/KYC, incluidos:

- proveedores de verificación de documentos;
- proveedores de prueba de vida;
- proveedores de screening de sanciones;
- proveedores de screening PEP/adverse media;
- proveedores de analítica blockchain;
- socios de pago;
- bancos, procesadores y proveedores de cambio;
- asesores legales, de cumplimiento y auditoría;
- proveedores de infraestructura y seguridad.

Los proveedores pueden indicarse por categorías sin nombres específicos, salvo que la ley, un contrato con el proveedor o una política separada de la Compañía disponga lo contrario.

La Compañía puede verificar a socios y proveedores en cuanto a sanciones, reputación, licencias, autorizaciones, riesgos y capacidad de cumplir requisitos de seguridad y confidencialidad.

16. Obligaciones del usuario

El usuario se compromete a:

- no utilizar la Plataforma para actividades prohibidas;
- proporcionar información veraz;
- responder oportunamente a las solicitudes de la Compañía;
- proporcionar documentos y explicaciones si se solicitan;
- utilizar únicamente fondos que le pertenezcan legalmente;
- no utilizar tarjetas bancarias, cuentas, billeteras o datos de pago de terceros sin base legal;
- no proporcionar documentos, recibos, capturas de pantalla o comprobantes falsificados;
- no eludir límites, verificaciones, restricciones de sanciones o reglas de la Plataforma;
- no crear múltiples cuentas para eludir restricciones;
- cumplir la legislación aplicable;
- evaluar de forma independiente la legalidad de sus operaciones en su país de residencia.

La negativa a cooperar, la evasión de verificación, la presentación de información falsa o el intento de eludir los controles AML/KYC puede dar lugar a la restricción o terminación del servicio.

17. Confidencialidad de los procedimientos AML/KYC

El usuario entiende que la Compañía no divulga:

- criterios exactos de riesgo;
- red flags internas;
- umbrales de monitoreo;
- algoritmos de scoring;
- fuentes de datos AML;
- detalles de investigaciones;
- razones para presentar un reporte ante autoridades competentes;
- detalles de decisiones internas;
- información cuya divulgación pueda infringir la ley, la seguridad o la eficacia de los controles AML/KYC.

18. Modificación de la Política

La Compañía puede modificar esta Política en cualquier momento. La versión vigente se publica en el sitio web <https://kashbi.io> o en la interfaz de la Plataforma.

El uso continuado de la Plataforma después de la publicación de una versión actualizada significa el consentimiento del usuario con la nueva versión de la Política, salvo que la legislación aplicable disponga lo contrario.

19. Versiones lingüísticas

La presente Política puede publicarse en ruso, kazajo, inglés y otros idiomas.

Si la legislación aplicable exige la prioridad de una versión lingüística determinada, se aplicará dicha versión. En los demás casos, en caso de discrepancias entre versiones lingüísticas, prevalecerá la versión rusa.

20. Contactos

Para cuestiones relacionadas con la presente Política, el usuario puede contactar:

- Compañía: F-Tech
- País de registro: Kazakhstan
- Sitio web: <https://kashbi.io>
- Aplicación: KashBi
- Email: legal@kashbi.io
- Telegram: [kashbi_support](#)
- Domicilio legal: 44/1 Al-Farabi Avenue, Apartment 207