

Política de Privacidad

La presente Política de Privacidad (la «Política») describe cómo F-Tech (la «Compañía», «nosotros», «nos», «nuestro») recopila, utiliza, almacena, transmite y protege los datos personales de los usuarios del sitio web <https://kashbi.io>, la aplicación KashBi, el bot de Telegram, la Telegram Mini App, la versión web, la API y otros servicios relacionados de la Compañía (en adelante, la «Plataforma»).

La Política se aplica a los usuarios, visitantes del sitio web, cuentas registradas, participantes en operaciones P2P, titulares de monederos, solicitantes que se comuniquen con el servicio de soporte y otras personas cuyos datos puedan ser tratados al utilizar la Plataforma.

La presente Política forma parte de los términos de usuario, las reglas de uso de la Plataforma, las políticas AML/KYC/CTF y otros documentos de la Compañía, cuando dichos documentos resulten aplicables. Si usted no está de acuerdo con la presente Política, por favor deje de utilizar la Plataforma.

1. Términos y definiciones

1.1. Datos personales: cualquier información relativa a una persona física identificada o identificable, directa o indirectamente.

1.2. Tratamiento de datos personales: cualquier operación o conjunto de operaciones realizadas sobre datos personales, incluida la recopilación, registro, organización, estructuración, acumulación, almacenamiento, rectificación, actualización, modificación, extracción, uso, transmisión, puesta a disposición, acceso, anonimización, bloqueo, supresión y destrucción.

1.3. Usuario: una persona física que visita el sitio web, se registra en la Plataforma, utiliza un monedero, participa en operaciones P2P, se comunica con soporte o interactúa de cualquier otro modo con la Plataforma.

1.4. Cuenta: la cuenta de usuario en la Plataforma, creada a través de la Telegram Mini App, el bot de Telegram, la versión web, la aplicación móvil u otro método disponible.

1.5. Activos digitales: criptomonedas, tokens, stablecoins y otras unidades digitales de cuenta admitidas por la Plataforma.

1.6. Operación P2P: una operación entre usuarios de la Plataforma en la que los usuarios acuerdan de forma independiente las condiciones de intercambio, pago, transmisión de activos digitales, fondos fiduciarios, bienes, servicios u otros valores, si dicha funcionalidad está prevista por la Plataforma.

1.7. AML/KYC/CTF: procedimientos de prevención del lavado de activos, financiación del terrorismo, evasión de sanciones, fraude y otras actividades prohibidas, así como procedimientos de identificación, verificación del usuario y evaluación de riesgos.

1.8. Encargado del tratamiento: un tercero que trata datos personales por cuenta de la Compañía, en interés de la Compañía o para garantizar el funcionamiento de la Plataforma.

2. Información sobre la Compañía y datos de contacto

F-Tech es el operador o la entidad responsable respecto de los datos personales tratados en relación con el uso de la Plataforma, salvo que se desprenda otra cosa de la legislación aplicable o de un servicio específico.

Datos de contacto:

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

3. Principios generales del tratamiento de datos personales

Procuramos tratar los datos personales de manera lícita, leal y transparente. Nos guiamos por los principios de licitud, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, seguridad y confidencialidad.

No procuramos recopilar más datos de los necesarios para el funcionamiento de la Plataforma, el cumplimiento de la ley, la seguridad, la prevención del fraude, la resolución de disputas, los procedimientos AML/KYC/CTF y la protección de los derechos de la Compañía y de los usuarios.

4. Bases jurídicas del tratamiento

Dependiendo de la finalidad concreta y de la legislación aplicable, podemos tratar datos personales sobre las siguientes bases:

- consentimiento del usuario;
- ejecución de un contrato o adopción de medidas precontractuales;
- cumplimiento de obligaciones legales;
- interés legítimo de la Compañía;
- protección de intereses vitales del usuario o de otras personas, cuando resulte aplicable.

Cuando el tratamiento se realice sobre la base del consentimiento, el usuario tendrá derecho a retirarlo. La retirada del consentimiento no afectará a la licitud del tratamiento realizado antes de dicha retirada y no impedirá el tratamiento de datos sobre otras bases jurídicas legítimas.

5. Datos que podemos tratar

5.1. Datos de cuenta y registro:

- Telegram ID;
- nombre de usuario de Telegram;
- nombre, apellido o nombre visible de Telegram, si Telegram los transmite;
- avatar o imagen de perfil, si está disponible a través de Telegram o si el usuario la carga;
- datos initData de Telegram WebApp necesarios para la autorización y la verificación de autenticidad del inicio de sesión;
- información sobre la vinculación de una cuenta de Telegram con una cuenta creada en la versión web;
- dirección de correo electrónico;
- número de teléfono;
- nombre de usuario;
- contraseña en forma de hash criptográfico para la versión web;
- código PIN en forma de hash criptográfico u otro valor técnico protegido para la Telegram Mini App;
- información sobre la activación y el uso de 2FA para la versión web;
- configuraciones biométricas únicamente como indicador técnico de activación de la función, sin recibir ni almacenar plantillas biométricas;
- otros factores de seguridad en forma de identificadores técnicos, hashes o indicadores de activación de la función;
- fecha de registro, estado de la cuenta, idioma de la interfaz, configuraciones de notificaciones;
- código de referencia, ID del usuario invitante o información sobre el programa de afiliados, si resulta aplicable.

5.2. Datos técnicos:

- dirección IP;
- ubicación aproximada determinada por la dirección IP;
- datos sobre el dispositivo, navegador, sistema operativo, versión de la aplicación e idioma;

- identificadores de sesión;
- información sobre inicios de sesión en la cuenta;
- registros de seguridad;
- datos sobre errores, fallas, eventos de la aplicación y diagnóstico;
- fecha, hora y duración del uso de la Plataforma;
- información sobre acciones del usuario en la interfaz necesaria para la seguridad, analítica y mejora del servicio.

5.3. Datos del monedero y de operaciones con activos digitales:

- identificadores internos de monederos y saldos;
- direcciones públicas de blockchain;
- memo, tag, comment u otros identificadores de pago;
- txid, hash de transacción, número de bloque, número de confirmaciones, red, activo, importe, comisión;
- direcciones del remitente y del destinatario en la blockchain;
- historial de depósitos, retiros, transferencias, transferencias internas, retenciones, bloqueos, reservas, congelaciones, reembolsos, comisiones y ajustes;
- información sobre el estado de la transacción;
- datos sobre el origen de los activos digitales recibidos, si son necesarios para el análisis AML o la verificación del origen de los fondos;
- resultados de la revisión automática o manual de riesgo de transacciones blockchain, si dicha revisión se aplica.

Los datos públicos de blockchain pueden estar disponibles en las redes blockchain correspondientes con independencia de la Compañía. La Compañía no controla los registros públicos de blockchain y no puede eliminar ni modificar datos ya registrados en una red blockchain pública.

5.4. Datos de operaciones P2P:

- ID del anuncio, oferta u operación;
- rol del usuario en la operación;
- tipo de operación;
- activo digital seleccionado, red y moneda de liquidación;
- importe, precio, tipo de cambio, margen, límites, comisiones;
- estado de la operación;
- fecha y hora de creación, aceptación, pago, confirmación, finalización, cancelación o apertura de disputa;
- condiciones de la operación, comentarios e instrucciones;

- método de pago;
- datos de pago que el usuario indique para ejecutar la operación;
- confirmaciones de pago, recibos, capturas de pantalla, comprobantes, mensajes, archivos adjuntos y otras pruebas;
- correspondencia entre los participantes de la operación, si dicha función está prevista;
- acciones de moderadores o árbitros en una disputa;
- resultado de la disputa y fundamentos de la decisión adoptada.

El usuario no debe transmitir a través del chat, la descripción de la operación, archivos adjuntos u otros campos datos personales excesivos, datos de terceros, códigos secretos, contraseñas, frases semilla, claves privadas u otra información confidencial que no sea necesaria para ejecutar la operación.

5.5. Datos de pagos fiduciarios

En el marco de las operaciones P2P, los pagos fiduciarios se realizan directamente entre los usuarios, salvo que un servicio separado de la Plataforma disponga expresamente otra cosa. La Compañía no es un banco, una entidad de pago ni parte de una transferencia fiduciaria entre usuarios; sin embargo, para garantizar las operaciones P2P, resolver disputas, prevenir el fraude y cumplir los requisitos aplicables, podemos tratar:

- método de pago seleccionado;
- nombre del titular de la cuenta o instrumento de pago, si lo proporciona el usuario;
- datos enmascarados de tarjeta o cuenta;
- banco, sistema de pago o proveedor;
- país del instrumento de pago;
- importe, moneda, fecha y estado del pago;
- identificador de pago del proveedor, si dicho identificador es proporcionado por el usuario;
- información sobre reembolso, cancelación, contracargo, disputa u operación sospechosa.

No debemos solicitar ni almacenar datos completos de tarjetas bancarias, códigos CVV/CVC, contraseñas de aplicaciones bancarias, códigos de confirmación de pagos u otros datos de pago secretos.

5.6. Datos AML/KYC/CTF y de evaluación de riesgos

Aplicamos un enfoque basado en riesgos para AML/KYC/CTF. La identificación, verificación, revisiones adicionales o solicitudes de documentos pueden no aplicarse por defecto a todos los usuarios, sino en los casos en que sea necesario teniendo en cuenta la legislación aplicable, las reglas internas de gestión de riesgos, límites, tipo de operación, indicios de actividad sospechosa, requisitos de socios, una disputa, una solicitud a soporte u otros factores de riesgo.

Si se aplican procedimientos AML/KYC/CTF al usuario, podemos tratar:

- nombre, apellido, segundo nombre u otro nombre completo;
- fecha de nacimiento;
- nacionalidad;
- país de residencia;
- domicilio de residencia;
- número de teléfono;
- email;
- documento de identidad;
- fotografía, selfie, verificación por video o prueba de vida;
- información sobre beneficiario final, origen de los fondos, origen del patrimonio, actividad profesional o propósito de las operaciones, si resulta aplicable;
- resultados de verificaciones de sanciones, PEP, adverse media y otras verificaciones;
- resultados de verificaciones AML de direcciones y transacciones blockchain;
- perfil interno de riesgo del usuario;
- documentos y explicaciones proporcionados por el usuario a solicitud de la Compañía;
- información sobre actividad sospechosa, inusual, prohibida o de alto riesgo.

El mero hecho de registrarse en la Plataforma no significa que el usuario esté obligado en todos los casos a completar una verificación KYC completa, salvo que se establezca otra cosa en la interfaz, en las condiciones de un servicio específico o en los requisitos aplicables.

5.7. Datos del servicio de soporte:

- datos de contacto;
- contenido de la solicitud;
- archivos adjuntos, capturas de pantalla, documentos y mensajes;
- historial de correspondencia;
- grabaciones de solicitudes, si el canal de comunicación correspondiente prevé grabación;
- información sobre la resolución de la solicitud;
- datos necesarios para confirmar la titularidad de la cuenta.

5.8. Datos de marketing y comunicaciones:

- consentimientos y bajas de comunicaciones;
- email, nombre de usuario de Telegram, Telegram ID u otro canal de comunicación;
- historial de notificaciones;

- preferencias de idioma y tipo de mensajes;
- estadísticas de entrega e interacción con los mensajes, si resulta aplicable.

Podemos enviar mensajes de servicio, informativos y de marketing relacionados con la Plataforma, la seguridad, actualizaciones, nuevas funciones, cambios en los términos, promociones u otras ofertas de la Compañía. No procuramos enviar al usuario mensajes excesivos, engañosos o intrusivos. El usuario puede darse de baja de las comunicaciones de marketing, si dicha baja está prevista por la legislación aplicable o por la interfaz de la Plataforma. Las notificaciones de servicio y jurídicamente relevantes pueden enviarse con independencia de la baja de los mensajes de marketing.

6. Finalidades del tratamiento de datos personales

Podemos tratar datos personales para:

- registrar y administrar la cuenta;
- autorizar, autenticar y restablecer el acceso;
- proporcionar el monedero y operaciones con activos digitales;
- procesar depósitos, retiros, transferencias internas, saldos, comisiones y confirmaciones;
- proporcionar funciones P2P, crear ofertas, abrir y finalizar operaciones;
- reservar, retener o liberar activos digitales;
- intercambiar mensajes y pruebas entre participantes de una operación;
- resolver disputas y arbitraje;
- registrar el método de pago y verificar confirmaciones de pago en disputas P2P;
- AML/KYC/CTF, control de sanciones y gestión de riesgos;
- monitorear transacciones y verificar direcciones blockchain;
- seguridad, prevención de fraude, multicuentas, spam, phishing, ataques y otras infracciones;
- soporte a usuarios;
- mejora de la Plataforma, corrección de errores, prueba de funciones y analítica;
- fines legales, gestión de reclamaciones y protección de los derechos de la Compañía.

7. Cookies y tecnologías similares

Podemos utilizar local storage, session storage, identificadores técnicos de sesión, registros del servidor, analítica propia no basada en cookies y otras tecnologías similares para autorización, conservación de configuraciones, protección de sesión, prevención de fraude, analítica, diagnóstico de errores, mejora del funcionamiento de la Plataforma y cumplimiento de requisitos de seguridad.

Si en el futuro la Compañía comienza a utilizar cookies o analítica de cookies de terceros, dicho tratamiento se reflejará en la presente Política, en una Política de Cookies separada

o en una interfaz de consentimiento, si así lo requiere la legislación aplicable.

8. Tratamiento automatizado y elaboración de perfiles

Podemos utilizar herramientas automatizadas y semiautomatizadas para analizar eventos técnicos, transacciones, riesgos AML, actividad sospechosa, infracciones de reglas, multicuentas y otros factores de seguridad.

La Plataforma se posiciona como privacy-first: procuramos minimizar la recopilación de datos personales, no solicitar documentos de identificación sin necesidad y utilizar un enfoque basado en riesgos para las verificaciones. Privacy-first no significa anonimato completo y no excluye el tratamiento de datos necesarios para la seguridad, el cumplimiento de la ley, los procedimientos AML/KYC/CTF, la resolución de disputas, la prevención del fraude y la protección de la Plataforma.

Dicho tratamiento puede afectar la disponibilidad de funciones individuales de la Plataforma, límites, la necesidad de verificación adicional, la suspensión de una operación o la remisión del caso a revisión manual.

9. Transferencia de datos a terceros

No vendemos los datos personales de los usuarios ni los transferimos a terceros para el marketing independiente de dichos terceros sin el consentimiento del usuario.

Podemos transferir datos personales a las siguientes categorías de destinatarios:

1. proveedores de infraestructura;
2. proveedores de servicios AML/KYC/CTF;
3. bancos, proveedores de pago y procesadores, únicamente si dichas personas participan en un servicio u operación concretos;
4. proveedores de analítica y diagnóstico;
5. proveedores de comunicaciones;
6. asesores jurídicos, de auditoría y de cumplimiento;
7. entidades vinculadas a la Compañía;
8. autoridades competentes;
9. contrapartes de una operación P2P, únicamente en la medida necesaria para ejecutar la operación;
10. sucesores potenciales o efectivos en caso de cambios corporativos.

En una operación P2P ordinaria, el pago fiduciario se realiza directamente entre los usuarios, y la Compañía no procesa el pago fiduciario como intermediario de pago.

10. Transferencia transfronteriza de datos

La Plataforma puede utilizar infraestructura, socios, contratistas y encargados del tratamiento ubicados en diferentes países. En consecuencia, los datos personales pueden

transferirse, almacenarse y tratarse fuera del país de residencia del usuario o del país de registro de la Compañía.

En caso de transferencia transfronteriza de datos, adoptamos medidas razonables para garantizar un nivel adecuado de protección de los datos personales, incluidas obligaciones contractuales de confidencialidad, medidas técnicas y organizativas de seguridad, revisión de proveedores y otros mecanismos previstos por la legislación aplicable.

11. Conservación de datos personales

Conservamos los datos personales durante el tiempo necesario para las finalidades para las que fueron recopilados, así como para cumplir obligaciones legales, resolver disputas, prevenir el fraude y proteger los derechos de la Compañía y de los usuarios.

Plazos orientativos de conservación:

1. datos de cuenta: durante la existencia de la cuenta y por un periodo razonable después de su cierre;
2. datos de transacciones, saldos, depósitos, retiros y operaciones P2P: al menos durante el plazo exigido por la legislación aplicable, reglas AML/CTF, requisitos contables o reglas internas de gestión de riesgos;
3. datos AML/KYC/CTF: durante el plazo establecido por la legislación aplicable;
4. datos de soporte: durante el plazo necesario para tramitar la solicitud, resolver una disputa, mejorar el servicio y proteger los derechos de la Compañía;
5. registros técnicos y datos de seguridad: durante el plazo necesario para la seguridad, diagnóstico, investigación de incidentes y prevención de abusos;
6. datos de marketing: hasta la retirada del consentimiento o la baja de comunicaciones, salvo que se requiera una conservación más prolongada para confirmar el hecho del consentimiento o de la baja.

La eliminación de la cuenta o la retirada del consentimiento no siempre implica la eliminación inmediata de todos los datos. Podemos conservar datos si ello es necesario para cumplir la ley, AML/KYC/CTF, contabilidad, prevención del fraude, resolución de disputas, cumplimiento de requisitos judiciales o regulatorios, o protección de los derechos de la Compañía.

12. Datos públicos de blockchain

El usuario entiende que las operaciones con activos digitales pueden registrarse en redes blockchain públicas o parcialmente públicas. La Compañía no es operadora de dichas redes, no controla su funcionamiento y no puede eliminar, ocultar, modificar ni limitar la difusión de información ya publicada en la blockchain.

13. Confidencialidad de la cuenta y responsabilidad del usuario

El usuario está obligado a garantizar por sí mismo la confidencialidad de los datos de acceso a la cuenta, incluida la contraseña de la versión web, el código PIN de la Telegram

Mini App, códigos 2FA, dispositivos, email, cuenta de Telegram y otros medios de autorización.

El usuario no debe transmitir a terceros la contraseña, el código PIN, códigos de un solo uso, códigos 2FA, frase semilla, claves privadas, códigos de respaldo, acceso al dispositivo o a la cuenta de Telegram, ni otros datos que permitan obtener acceso a la cuenta o a los activos digitales.

La Compañía no solicita frases semilla, claves privadas, datos completos de tarjetas bancarias, códigos CVV/CVC ni contraseñas de servicios de terceros.

14. Datos de terceros

El usuario no debe transmitir a la Compañía datos personales de terceros sin una base legal y el consentimiento de dichas personas, si tal consentimiento es requerido. Si el usuario transmite datos de terceros en el marco de una operación P2P, una solicitud de soporte, una disputa, la carga de documentos u otra interacción con la Plataforma, el usuario confirma que tiene derecho a transmitir dichos datos.

15. Derechos del usuario

Dependiendo de la legislación aplicable, el usuario puede tener derecho a:

- acceder a los datos personales;
- recibir una copia de los datos;
- rectificar datos inexactos, incompletos u obsoletos;
- suprimir datos;
- limitar el tratamiento;
- oponerse al tratamiento;
- la portabilidad de los datos;
- retirar el consentimiento;
- presentar una reclamación ante una autoridad supervisora competente.

Podemos denegar la supresión total o parcial de datos si su conservación es necesaria para cumplir la ley, obligaciones AML/KYC/CTF, contabilidad, prevención del fraude, resolución de disputas, ejecución de contratos o protección de los derechos de la Compañía.

16. Seguridad de los datos personales

Aplicamos medidas técnicas y organizativas razonables para proteger los datos personales, incluido el cifrado de la transmisión de datos, control de acceso, separación de permisos, registro de acciones, monitoreo de actividad sospechosa, copias de seguridad, procedimientos de respuesta a incidentes y reglas internas de seguridad de la información.

A pesar de las medidas adoptadas, ningún método de transmisión de datos por internet ni

ningún sistema de almacenamiento es absolutamente seguro. El usuario debe cumplir las medidas de seguridad por su parte.

17. Niños y menores de edad

La Plataforma no está destinada a personas que no hayan alcanzado la edad mínima necesaria para utilizar de forma autónoma los servicios correspondientes en el país de residencia del usuario.

18. Enlaces a recursos de terceros

La Plataforma puede contener enlaces a sitios web, aplicaciones, monederos, exploradores de blockchain, servicios de pago, recursos de Telegram u otros servicios externos de terceros. La Compañía no controla dichos recursos de terceros y no es responsable de sus políticas de privacidad, seguridad, contenido ni tratamiento de datos.

19. Modificaciones de la Política

Podemos modificar periódicamente la presente Política para reflejar cambios en la Plataforma, la legislación, requisitos de socios, tecnologías, riesgos o procesos internos. La versión vigente de la Política se publica en el sitio web <https://kashbi.io> o en la interfaz de la Plataforma.

20. Contacto con nosotros

Para cuestiones relativas a la presente Política, el tratamiento de datos personales, el ejercicio de los derechos del usuario o reclamaciones, el usuario puede comunicarse con:

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

21. Versiones lingüísticas

El presente documento puede publicarse en diferentes idiomas. Si la legislación aplicable exige la prioridad de una determinada versión lingüística, se aplicará dicha versión. En los demás casos, en caso de discrepancias entre versiones lingüísticas, prevalecerá la versión en inglés.