

Política de Privacidade

A presente Política de Privacidade (“Política”) descreve como F-Tech (“Empresa”, “nós”, “nos”, “nosso”) recolhe, utiliza, armazena, transmite e protege os dados pessoais dos utilizadores do site <https://kashbi.io>, da aplicação KashBi, do bot do Telegram, do Telegram Mini App, da versão web, da API e de outros serviços relacionados da Empresa (doravante, a “Plataforma”).

A Política aplica-se aos utilizadores, visitantes do site, contas registadas, participantes em transações P2P, titulares de carteiras, requerentes junto do suporte e outras pessoas cujos dados possam ser tratados durante a utilização da Plataforma.

A presente Política faz parte dos termos de utilização, regras de uso da Plataforma, políticas AML/KYC/CTF e outros documentos da Empresa, se tais documentos forem aplicáveis. Se não concordar com a presente Política, por favor, cesse a utilização da Plataforma.

1. Termos e definições

1.1. Dados pessoais — qualquer informação relativa a uma pessoa singular identificada ou identificável, direta ou indiretamente.

1.2. Tratamento de dados pessoais — qualquer operação ou conjunto de operações realizadas sobre dados pessoais, incluindo recolha, registo, organização, estruturação, acumulação, conservação, retificação, atualização, alteração, extração, utilização, transmissão, disponibilização de acesso, anonimização, bloqueio, apagamento e destruição.

1.3. Utilizador — pessoa singular que visita o site, se regista na Plataforma, utiliza a carteira, participa em transações P2P, contacta o suporte ou interage de qualquer outra forma com a Plataforma.

1.4. Conta — conta de utilizador na Plataforma, criada através do Telegram Mini App, do bot do Telegram, da versão web, da aplicação móvel ou de outro método disponível.

1.5. Ativos digitais — criptomoedas, tokens, stablecoins e outras unidades digitais de conta suportadas pela Plataforma.

1.6. Transação P2P — transação entre utilizadores da Plataforma, no âmbito da qual os utilizadores acordam de forma independente as condições de troca, pagamento, transferência de ativos digitais, fundos fiduciários, bens, serviços ou outros valores, se tal funcionalidade for disponibilizada pela Plataforma.

1.7. AML/KYC/CTF — procedimentos de combate ao branqueamento de capitais, ao financiamento do terrorismo, à evasão de sanções, à fraude e a outras atividades proibidas, bem como procedimentos de identificação, verificação do utilizador e avaliação de risco.

1.8. Subcontratante — terceiro que trata dados pessoais por conta da Empresa, no interesse da Empresa ou para assegurar o funcionamento da Plataforma.

2. Sobre a Empresa e contactos

A Empresa F-Tech é a operadora ou outra entidade responsável pelos dados pessoais tratados em ligação com a utilização da Plataforma, salvo se o contrário resultar da legislação aplicável ou de um serviço específico.

Contactos:

- Site: <https://kashbi.io>
- Aplicação: KashBi
- Email de suporte: legal@kashbi.io
- Suporte no Telegram: [kashbi_support](https://t.me/kashbi_support)
- País de registo: Kazakhstan
- Endereço legal: 44/1 Al-Farabi Avenue, Apartment 207

3. Princípios gerais do tratamento de dados pessoais

Procuramos tratar os dados pessoais de forma lícita, leal e transparente. Orientamo-nos pelos princípios da licitude, limitação das finalidades, minimização dos dados, exatidão, limitação da conservação, segurança e confidencialidade.

Não procuramos recolher mais dados do que o necessário para o funcionamento da Plataforma, o cumprimento da lei, a segurança, a prevenção de fraude, a resolução de litígios, os procedimentos AML/KYC/CTF e a proteção dos direitos da Empresa e dos utilizadores.

4. Fundamentos legais do tratamento

Dependendo da finalidade específica e da legislação aplicável, podemos tratar dados pessoais com base nos seguintes fundamentos:

- consentimento do utilizador;
- execução de um contrato ou adoção de medidas pré-contratuais;
- cumprimento de obrigações legais;
- interesse legítimo da Empresa;
- proteção dos interesses vitais do utilizador ou de outras pessoas, quando aplicável.

Quando o tratamento se basear no consentimento, o utilizador tem o direito de retirar esse consentimento. A retirada do consentimento não afeta a licitude do tratamento realizado antes dessa retirada e não impede o tratamento dos dados com base em outros fundamentos legais.

5. Dados que podemos tratar

5.1. Dados de conta e registo:

- Telegram ID;
- nome de utilizador do Telegram;
- nome, apelido/sobrenome ou nome de exibição do Telegram, se transmitidos pelo Telegram;
- avatar ou imagem de perfil, se disponível através do Telegram ou carregado pelo utilizador;
- dados Telegram WebApp initData necessários para autorização e verificação da autenticidade do acesso;
- informações sobre a vinculação da conta Telegram a uma conta criada na versão web;
- endereço de email;
- número de telefone;
- login;
- palavra-passe sob a forma de hash criptográfico para a versão web;
- código PIN sob a forma de hash criptográfico ou outro valor técnico protegido para o Telegram Mini App;
- informações sobre a ativação e utilização de 2FA para a versão web;
- definições biométricas apenas sob a forma de indicador técnico de ativação da função, sem recolha ou conservação de modelos biométricos;
- outros fatores de segurança sob a forma de identificadores técnicos, hashes ou indicadores de ativação de função;
- data de registo, estado da conta, idioma da interface, definições de notificações;
- código de referência, ID do utilizador que convidou ou informações sobre programa de parceiros, quando aplicável.

5.2. Dados técnicos:

- endereço IP;
- localização aproximada determinada pelo endereço IP;
- dados sobre dispositivo, navegador, sistema operativo, versão da aplicação e idioma;
- identificadores de sessão;
- informações sobre acessos à conta;
- registos de segurança;
- dados sobre erros, falhas, eventos da aplicação e diagnóstico;

- data, hora e duração da utilização da Plataforma;
- informações sobre ações do utilizador na interface, necessárias para segurança, análise e melhoria do serviço.

5.3. Dados de carteira e operações com ativos digitais:

- identificadores internos de carteiras e saldos;
- endereços públicos de blockchain;
- memo, tag, comentário ou outros identificadores de pagamento;
- txid, hash da transação, número do bloco, número de confirmações, rede, ativo, montante, comissão/taxa;
- endereços do remetente e do destinatário na blockchain;
- histórico de depósitos, levantamentos/saques, transferências, transferências internas, retenções, bloqueios, reservas, congelamentos, reembolsos, comissões/taxas e ajustes;
- informações sobre o estado da transação;
- dados sobre a origem dos ativos digitais recebidos, se necessários para análise AML ou verificação da origem dos fundos;
- resultados de verificações automáticas ou manuais de risco de transações em blockchain, se tal verificação for aplicada.

Os dados públicos de blockchain podem estar disponíveis nas redes blockchain correspondentes independentemente da Empresa. A Empresa não controla registos públicos de blockchain e não pode apagar ou alterar dados já registados numa rede blockchain pública.

5.4. Dados de transações P2P:

- ID do anúncio, oferta ou transação;
- papel do utilizador na transação;
- tipo de transação;
- ativo digital, rede e moeda de liquidação selecionados;
- montante, preço, taxa de câmbio, margem, limites, comissões/taxas;
- estado da transação;
- data e hora de criação, aceitação, pagamento, confirmação, conclusão, cancelamento ou abertura de litígio;
- condições da transação, comentários e instruções;
- método de pagamento;
- dados de pagamento que o utilizador indica para a execução da transação;
- confirmações de pagamento, recibos, capturas de ecrã/tela, comprovativos, mensagens, anexos e outras provas;

- correspondência entre participantes da transação, se tal função for disponibilizada;
- ações de moderadores ou árbitros no litígio;
- resultado do litígio e fundamentos da decisão tomada.

O utilizador não deve transmitir através do chat, da descrição da transação, de anexos ou de outros campos dados pessoais excessivos, dados de terceiros, códigos secretos, palavras-passe, seed phrases, chaves privadas ou outras informações confidenciais que não sejam necessárias para a execução da transação.

5.5. Dados de pagamentos fiduciários

No âmbito das transações P2P, os pagamentos fiduciários são realizados diretamente entre utilizadores, salvo se expressamente previsto de outra forma por um serviço separado da Plataforma. A Empresa não é banco, instituição de pagamento ou parte na transferência fiduciária entre utilizadores; contudo, para assegurar transações P2P, resolver litígios, prevenir fraude e cumprir requisitos aplicáveis, podemos tratar:

- método de pagamento selecionado;
- nome do titular da conta ou do instrumento de pagamento, se fornecido pelo utilizador;
- dados mascarados do cartão ou da conta;
- banco, sistema de pagamento ou provedor;
- país do instrumento de pagamento;
- montante, moeda, data e estado do pagamento;
- identificador de pagamento junto do provedor, se tal identificador for fornecido pelo utilizador;
- informações sobre reembolso, cancelamento, chargeback, litígio ou operação suspeita.

Não devemos solicitar nem conservar dados completos de cartões bancários, códigos CVV/CVC, palavras-passe de aplicações bancárias, códigos de confirmação de pagamentos ou outros dados secretos de pagamento.

5.6. Dados AML/KYC/CTF e de avaliação de risco

Aplicamos uma abordagem baseada no risco a AML/KYC/CTF. Identificação, verificação, verificações adicionais ou solicitação de documentos podem não ser aplicadas por defeito a todos os utilizadores, mas apenas nos casos em que tal seja necessário tendo em conta a legislação aplicável, regras internas de gestão de risco, limites, tipo de operação, indícios de atividade suspeita, requisitos de parceiros, litígio, pedido ao suporte ou outros fatores de risco.

Se forem aplicados procedimentos AML/KYC/CTF ao utilizador, podemos tratar:

- nome, apelido/sobrenome, patronímico ou outro nome completo;
- data de nascimento;
- nacionalidade;
- país de residência;

- endereço de residência;
- número de telefone;
- email;
- documento de identificação;
- fotografia, selfie, verificação por vídeo ou verificação de vivacidade/liveness;
- informações sobre beneficiário efetivo, origem dos fundos, origem do património, atividade profissional ou finalidade das operações, quando aplicável;
- resultados de verificações de sanções, PEP, adverse media e outras verificações;
- resultados de verificações AML de endereços e transações em blockchain;
- perfil interno de risco do utilizador;
- documentos e explicações fornecidos pelo utilizador a pedido da Empresa;
- informações sobre atividade suspeita, incomum, proibida ou de alto risco.

O simples facto de se registar na Plataforma não significa que o utilizador seja sempre obrigado a passar por verificação KYC completa, salvo se o contrário for previsto pela interface, pelos termos de um serviço específico ou por requisitos aplicáveis.

5.7. Dados do suporte:

- dados de contacto;
- conteúdo do pedido;
- anexos, capturas de ecrã/tela, documentos e mensagens;
- histórico de correspondência;
- gravações de pedidos, se o canal de comunicação correspondente prever gravação;
- informações sobre a resolução do pedido;
- dados necessários para confirmar a titularidade da conta.

5.8. Dados de marketing e comunicações:

- consentimentos e recusas de comunicações;
- email, nome de utilizador do Telegram, Telegram ID ou outro canal de comunicação;
- histórico de notificações;
- preferências de idioma e tipo de mensagens;
- estatísticas de entrega e interação com mensagens, quando aplicável.

Podemos enviar mensagens de serviço, informativas e de marketing relacionadas com a Plataforma, segurança, atualizações, novas funcionalidades, alterações de termos, promoções ou outras ofertas da Empresa. Não procuramos enviar ao utilizador mensagens excessivas, enganosas ou intrusivas. O utilizador pode cancelar a receção de comunicações de marketing, se tal cancelamento for previsto pela legislação aplicável ou

pela interface da Plataforma. Notificações de serviço e juridicamente relevantes podem ser enviadas independentemente da recusa de comunicações de marketing.

6. Finalidades do tratamento de dados pessoais

Podemos tratar dados pessoais para:

- registo e gestão da conta;
- autorização, autenticação e recuperação de acesso;
- disponibilização da carteira e de operações com ativos digitais;
- processamento de depósitos, levantamentos/saques, transferências internas, saldos, comissões/taxas e confirmações;
- disponibilização de funções P2P, criação de ofertas, abertura e conclusão de transações;
- reserva, retenção ou libertação de ativos digitais;
- troca de mensagens e provas entre participantes da transação;
- resolução de litígios e arbitragem;
- registo do método de pagamento e verificação de confirmações de pagamento em litígios P2P;
- AML/KYC/CTF, controlo de sanções e gestão de risco;
- monitorização de transações e verificação de endereços de blockchain;
- segurança, prevenção de fraude, multi-contas, spam, phishing, ataques e outras violações;
- suporte aos utilizadores;
- melhoria da Plataforma, correção de erros, teste de funcionalidades e análise;
- finalidades jurídicas, resolução de reclamações e proteção dos direitos da Empresa.

7. Cookies e tecnologias semelhantes

Podemos utilizar local storage, session storage, identificadores técnicos de sessão, registos de servidor, análises próprias não baseadas em cookies e outras tecnologias semelhantes para autorização, conservação de definições, proteção da sessão, prevenção de fraude, análise, diagnóstico de erros, melhoria do funcionamento da Plataforma e cumprimento de requisitos de segurança.

Se, no futuro, a Empresa começar a utilizar cookies ou análises de cookies de terceiros, esse tratamento será refletido na presente Política, numa Política de Cookies separada ou numa interface de consentimento, se tal for exigido pela legislação aplicável.

8. Tratamento automatizado e definição de perfis

Podemos utilizar meios automatizados e semiautomatizados para analisar eventos técnicos, transações, riscos AML, atividade suspeita, violações de regras, multi-contas e

outros fatores de segurança.

A Plataforma é posicionada como privacy-first: procuramos minimizar a recolha de dados pessoais, não solicitar documentos de identificação sem necessidade e utilizar uma abordagem baseada no risco para verificações. Privacy-first não significa anonimato absoluto e não exclui o tratamento de dados necessário para segurança, cumprimento da lei, procedimentos AML/KYC/CTF, resolução de litígios, prevenção de fraude e proteção da Plataforma.

Esse tratamento pode afetar a disponibilidade de determinadas funções da Plataforma, limites, necessidade de verificação adicional, suspensão de uma operação ou encaminhamento do caso para revisão manual.

9. Transferência de dados a terceiros

Não vendemos dados pessoais dos utilizadores e não os transmitimos a terceiros para marketing próprio desses terceiros sem o consentimento do utilizador.

Podemos transmitir dados pessoais às seguintes categorias de destinatários:

1. fornecedores de infraestrutura;
2. fornecedores de serviços AML/KYC/CTF;
3. bancos, provedores de pagamento e processadores, apenas se tais entidades participarem num serviço ou operação específico;
4. fornecedores de análise e diagnóstico;
5. fornecedores de comunicações;
6. consultores jurídicos, de auditoria e de compliance;
7. entidades relacionadas com a Empresa;
8. autoridades competentes;
9. contrapartes em transações P2P — apenas na medida necessária para a execução da transação;
10. sucessores potenciais ou efetivos em caso de alterações societárias.

Numa transação P2P comum, o pagamento fiduciário é realizado diretamente entre utilizadores, e a Empresa não trata o pagamento fiduciário como intermediário de pagamento.

10. Transferência transfronteiriça de dados

A Plataforma pode utilizar infraestrutura, parceiros, contratados e subcontratantes localizados em diferentes países. Em razão disso, os dados pessoais podem ser transferidos, armazenados e tratados fora do país de residência do utilizador ou do país de registo da Empresa.

Em caso de transferência transfronteiriça de dados, adotamos medidas razoáveis para assegurar um nível adequado de proteção dos dados pessoais, incluindo obrigações contratuais de confidencialidade, medidas técnicas e organizacionais de segurança,

verificação de fornecedores e outros mecanismos previstos pela legislação aplicável.

11. Conservação de dados pessoais

Conservamos os dados pessoais pelo período necessário às finalidades para as quais foram recolhidos, bem como para cumprir obrigações legais, resolver litígios, prevenir fraude e proteger os direitos da Empresa e dos utilizadores.

Prazos indicativos de conservação:

1. dados de conta — durante o período de existência da conta e por um período razoável após o seu encerramento;
2. dados de transações, saldos, depósitos, levantamentos/saques e transações P2P — pelo menos durante o período exigido pela legislação aplicável, regras AML/CTF, requisitos contabilísticos ou regras internas de gestão de risco;
3. dados AML/KYC/CTF — durante o período estabelecido pela legislação aplicável;
4. dados de suporte — durante o período necessário para tratar o pedido, resolver litígio, melhorar o serviço e proteger os direitos da Empresa;
5. registos técnicos e dados de segurança — durante o período necessário para segurança, diagnóstico, investigação de incidentes e prevenção de abusos;
6. dados de marketing — até à retirada do consentimento ou cancelamento da subscrição, salvo se for necessária conservação mais longa para comprovar o consentimento ou a recusa.

A eliminação da conta ou a retirada do consentimento nem sempre implica a eliminação imediata de todos os dados. Podemos conservar dados se isso for necessário para cumprir a lei, AML/KYC/CTF, contabilidade, prevenção de fraude, resolução de litígios, cumprimento de requisitos judiciais ou regulatórios ou proteção dos direitos da Empresa.

12. Dados públicos de blockchain

O utilizador compreende que as operações com ativos digitais podem ser registadas em redes blockchain públicas ou parcialmente públicas. A Empresa não é operadora dessas redes, não controla o seu funcionamento e não pode apagar, ocultar, alterar ou limitar a disseminação de informações já publicadas na blockchain.

13. Confidencialidade da conta e responsabilidade do utilizador

O utilizador é responsável por assegurar de forma independente a confidencialidade dos dados de acesso à conta, incluindo palavra-passe da versão web, código PIN do Telegram Mini App, códigos 2FA, dispositivos, email, conta Telegram e outros meios de autorização.

O utilizador não deve transmitir a terceiros palavra-passe, código PIN, códigos de uso único, códigos 2FA, seed phrase, chaves privadas, códigos de recuperação, acesso ao dispositivo ou à conta Telegram, bem como outros dados que permitam obter acesso à conta ou aos ativos digitais.

A Empresa não solicita seed phrases, chaves privadas, dados completos de cartões

bancários, códigos CVV/CVC ou palavras-passe de serviços de terceiros.

14. Dados de terceiros

O utilizador não deve transmitir à Empresa dados pessoais de terceiros sem fundamento legal e consentimento dessas pessoas, se tal consentimento for exigido. Se o utilizador transmitir dados de terceiros no âmbito de uma transação P2P, pedido ao suporte, litígio, carregamento de documentos ou outra interação com a Plataforma, o utilizador confirma que tem o direito de transmitir tais dados.

15. Direitos do utilizador

Dependendo da legislação aplicável, o utilizador pode ter direito:

- de acesso aos dados pessoais;
- de obter uma cópia dos dados;
- de retificação de dados inexatos, incompletos ou desatualizados;
- de apagamento dos dados;
- de limitação do tratamento;
- de oposição ao tratamento;
- de portabilidade dos dados;
- de retirada do consentimento;
- de apresentar reclamação a uma autoridade de controlo competente.

Podemos recusar a eliminação total ou parcial dos dados se a conservação for necessária para cumprir a lei, obrigações AML/KYC/CTF, contabilidade, prevenção de fraude, resolução de litígios, execução de contratos ou proteção dos direitos da Empresa.

16. Segurança dos dados pessoais

Aplicamos medidas técnicas e organizacionais razoáveis para proteger os dados pessoais, incluindo encriptação da transmissão de dados, controlo de acesso, segregação de permissões, registo de ações, monitorização de atividade suspeita, cópias de segurança, procedimentos de resposta a incidentes e regras internas de segurança da informação.

Apesar das medidas adotadas, nenhum método de transmissão de dados pela internet e nenhum sistema de armazenamento são absolutamente seguros. O utilizador deve cumprir medidas de segurança do seu lado.

17. Crianças e menores

A Plataforma não se destina a pessoas que não tenham atingido a idade mínima necessária para utilizar autonomamente os serviços correspondentes no país de residência do utilizador.

18. Ligações para recursos de terceiros

A Plataforma pode conter ligações para sites, aplicações, carteiras, exploradores de blockchain, serviços de pagamento, recursos do Telegram ou outros serviços externos de terceiros. A Empresa não controla tais recursos de terceiros e não é responsável pelas suas políticas de privacidade, segurança, conteúdo ou tratamento de dados.

19. Alteração da Política

Podemos alterar periodicamente a presente Política para refletir alterações na Plataforma, na legislação, nos requisitos de parceiros, nas tecnologias, nos riscos ou nos processos internos. A versão atual da Política é publicada no site <https://kashbi.io> ou na interface da Plataforma.

20. Contacte-nos

Para questões relativas à presente Política, ao tratamento de dados pessoais, ao exercício dos direitos do utilizador ou a reclamações, o utilizador pode contactar:

- Empresa: F-Tech
- País de registo: Kazakhstan
- Site: <https://kashbi.io>
- Aplicação: KashBi
- Email: legal@kashbi.io
- Telegram: [kashbi_support](#)
- Endereço legal: 44/1 Al-Farabi Avenue, Apartment 207

21. Versões linguísticas

O presente documento pode ser publicado em diferentes idiomas. Se a legislação aplicável exigir a prioridade de uma determinada versão linguística, essa versão será aplicável. Nos demais casos, em caso de divergências entre versões linguísticas, prevalecerá a versão em inglês.