

Політика конфіденційності

Ця Політика конфіденційності («Політика») описує, як F-Tech («Компанія», «ми», «нас», «наш») збирає, використовує, зберігає, передає та захищає персональні дані користувачів сайту <https://kashbi.io>, застосунку KashBi, Telegram-бота, Telegram Mini App, веб-версії, API та інших пов'язаних сервісів Компанії (далі — «Платформа»).

Політика застосовується до користувачів, відвідувачів сайту, зареєстрованих акаунтів, учасників P2P-угод, власників гаманців, заявників до служби підтримки та інших осіб, чії дані можуть оброблятися під час використання Платформи.

Ця Політика є частиною користувацьких умов, правил використання Платформи, AML/KYC/CTF-політик та інших документів Компанії, якщо такі документи застосовуються. Якщо ви не згодні з цією Політикою, будь ласка, припиніть використання Платформи.

1. Терміни та визначення

1.1. Персональні дані — будь-яка інформація, що стосується прямо або опосередковано ідентифікованої чи ідентифікуваної фізичної особи.

1.2. Обробка персональних даних — будь-яка дія або сукупність дій з персональними даними, включно зі збиранням, записом, систематизацією, накопиченням, зберіганням, уточненням, оновленням, зміною, вилученням, використанням, передачею, наданням доступу, знеособленням, блокуванням, видаленням і знищенням.

1.3. Користувач — фізична особа, яка відвідує сайт, реєструється на Платформі, використовує гаманець, бере участь у P2P-угодах, звертається до служби підтримки або іншим чином взаємодіє з Платформою.

1.4. Акаунт — обліковий запис користувача на Платформі, створений через Telegram Mini App, Telegram-бота, веб-версію, мобільний застосунок або інший доступний спосіб.

1.5. Цифрові активи — криптовалюти, токени, стейблкоїни та інші цифрові одиниці обліку, що підтримуються Платформою.

1.6. P2P-угода — угода між користувачами Платформи, у межах якої користувачі самостійно погоджують умови обміну, оплати, передання цифрових активів, фіатних коштів, товарів, послуг або інших цінностей, якщо така функціональність передбачена Платформою.

1.7. AML/KYC/CTF — процедури протидії відмиванню доходів, фінансуванню тероризму, обходу санкцій, шахрайству та іншій забороненій діяльності, а також процедури ідентифікації, перевірки користувача та оцінки ризику.

1.8. Обробник — третя особа, яка обробляє персональні дані за дорученням Компанії, в інтересах Компанії або для забезпечення роботи Платформи.

2. Про Компанію та контакти

Компанія F-Tech є оператором або іншою відповідальною особою щодо персональних даних, які обробляються у зв'язку з використанням Платформи, якщо інше не впливає із застосовного законодавства або конкретного сервісу.

Контакти:

- Сайт: <https://kashbi.io>
- Застосунок: KashBi
- Email підтримки: legal@kashbi.io
- Telegram-підтримка: [kashbi_support](https://t.me/kashbi_support)
- Країна реєстрації: Kazakhstan
- Юридична адреса: 44/1 Al-Farabi Avenue, Apartment 207

3. Загальні принципи обробки персональних даних

Ми прагнемо обробляти персональні дані законно, добросовісно та прозоро. Ми керуємося принципами законності, обмеження цілей, мінімізації даних, точності, обмеження строку зберігання, безпеки та конфіденційності.

Ми не прагнемо збирати більше даних, ніж необхідно для роботи Платформи, дотримання закону, безпеки, запобігання шахрайству, вирішення спорів, AML/KYC/CTF-процедур та захисту прав Компанії і користувачів.

4. Правові підстави обробки

Залежно від конкретної мети та застосовного законодавства ми можемо обробляти персональні дані на таких підставах:

- згода користувача;
- виконання договору або вжиття заходів до укладення договору;
- дотримання юридичних обов'язків;
- законний інтерес Компанії;
- захист життєво важливих інтересів користувача або інших осіб, якщо це застосовно.

Якщо обробка здійснюється на підставі згоди, користувач має право відкликати згоду. Відкликання згоди не впливає на законність обробки, здійсненої до такого відкликання, і не перешкоджає обробці даних на інших законних підставах.

5. Які дані ми можемо обробляти

5.1. Дані акаунта та реєстрації:

- Telegram ID;
- Telegram username;
- ім'я, прізвище або відображуване ім'я з Telegram, якщо вони передаються Telegram;
- аватар або зображення профілю, якщо воно доступне через Telegram або завантажене користувачем;
- дані Telegram WebApp initData, необхідні для авторизації та перевірки справжності входу;
- відомості про прив'язку Telegram-акаунта до акаунта, створеного у web-версії;
- адреса електронної пошти;
- номер телефону;
- логін;
- пароль у вигляді криптографічного хешу для web-версії;
- PIN-код у вигляді криптографічного хешу або іншого захищеного технічного значення для Telegram Mini App;
- відомості про ввімкнення та використання 2FA для web-версії;
- біометричні налаштування лише у вигляді технічної ознаки ввімкнення функції, без отримання та зберігання біометричних шаблонів;
- інші фактори безпеки у вигляді технічних ідентифікаторів, хешів або ознак ввімкнення функції;
- дата реєстрації, статус акаунта, мова інтерфейсу, налаштування сповіщень;
- реферальний код, ID користувача, який запросив, або відомості про партнерську програму, якщо застосовно.

5.2. Технічні дані:

- IP-адреса;
- приблизне місцезнаходження, визначене за IP-адресою;
- дані про пристрій, браузер, операційну систему, версію застосунку та мову;
- ідентифікатори сесії;
- відомості про входи в акаунт;
- журнали безпеки;
- дані про помилки, збої, події застосунку та діагностику;
- дата, час і тривалість використання Платформи;

- відомості про дії користувача в інтерфейсі, необхідні для безпеки, аналітики та покращення сервісу.

5.3. Дані гаманця та операцій із цифровими активами:

- внутрішні ідентифікатори гаманців і балансів;
- публічні блокчейн-адреси;
- memo, tag, comment або інші ідентифікатори платежу;
- txid, хеш транзакції, номер блоку, кількість підтверджень, мережа, актив, сума, комісія;
- адреси відправника та отримувача в блокчейні;
- історія депозитів, виведень, переказів, внутрішніх переказів, утримань, блокувань, резервування, заморожування, повернень, комісій і коригувань;
- відомості про статус транзакції;
- дані про джерело надходження цифрових активів, якщо вони необхідні для AML-аналізу або перевірки походження коштів;
- результати автоматичної або ручної перевірки блокчейн-транзакцій на ризик, якщо така перевірка застосовується.

Публічні блокчейн-дані можуть бути доступні у відповідних блокчейн-мережах незалежно від Компанії. Компанія не контролює публічні блокчейн-реєстри та не може видалити або змінити дані, вже записані в публічну блокчейн-мережу.

5.4. Дані P2P-угоди:

- ID оголошення, офера або угоди;
- роль користувача в угоді;
- тип угоди;
- вибраний цифровий актив, мережа та валюта розрахунку;
- сума, ціна, курс, маржа, ліміти, комісії;
- статус угоди;
- дата і час створення, прийняття, оплати, підтвердження, завершення, скасування або відкриття спору;
- умови угоди, коментарі та інструкції;
- платіжний метод;
- реквізити, які користувач зазначає для виконання угоди;
- підтвердження оплати, квитанції, скриншоти, чеки, повідомлення, вкладення та інші докази;
- листування між учасниками угоди, якщо така функція передбачена;
- дії модераторів або арбітрів у спорі;

- результат спору та підстави прийнятого рішення.

Користувач не повинен передавати через чат, опис угоди, вкладення або інші поля надмірні персональні дані, дані третіх осіб, секретні коди, паролі, seed-фрази, приватні ключі або іншу конфіденційну інформацію, яка не потрібна для виконання угоди.

5.5. Дані фіатних платежів

У межах P2P-угод фіатні платежі здійснюються безпосередньо між користувачами, якщо інше прямо не передбачено окремим сервісом Платформи. Компанія не є банком, платіжною організацією або стороною фіатного переказу між користувачами, однак для забезпечення P2P-угод, вирішення спорів, запобігання шахрайству та дотримання застосовних вимог ми можемо обробляти:

- вибраний платіжний метод;
- ім'я власника рахунку або платіжного інструменту, якщо воно надане користувачем;
- замасковані реквізити картки або рахунку;
- банк, платіжну систему або провайдера;
- країну платіжного інструменту;
- суму, валюту, дату та статус платежу;
- ідентифікатор платежу у провайдера, якщо такий ідентифікатор наданий користувачем;
- відомості про повернення, скасування, чарджбек, спір або підозрілу операцію.

Ми не повинні запитувати або зберігати повні дані банківських карток, CVV/CVC-коди, паролі від банківських застосунків, коди підтвердження платежів або інші секретні платіжні дані.

5.6. Дані AML/KYC/CTF та оцінки ризику

Ми застосовуємо ризик-орієнтований підхід до AML/KYC/CTF. Ідентифікація, верифікація, додаткові перевірки або запит документів можуть застосовуватися не до всіх користувачів за замовчуванням, а у випадках, коли це необхідно з урахуванням застосовного законодавства, внутрішніх правил управління ризиками, лімітів, типу операції, ознак підозрілої активності, вимог партнерів, спору, звернення до служби підтримки або інших факторів ризику.

Якщо до користувача застосовуються AML/KYC/CTF-процедури, ми можемо обробляти:

- ім'я, прізвище, по батькові або інше повне ім'я;
- дату народження;
- громадянство;
- країну проживання;
- адресу проживання;

- номер телефону;
- email;
- документ, що посвідчує особу;
- фотографію, селфі, відеоперевірку або liveness-перевірку;
- відомості про бенефіціарного власника, джерело коштів, джерело статків, рід діяльності або мету операцій, якщо застосовно;
- санкційні, PEP, adverse media та інші результати перевірок;
- результати AML-перевірки блокчейн-адрес і транзакцій;
- внутрішній ризик-профіль користувача;
- документи та пояснення, надані користувачем за запитом Компанії;
- відомості про підозрілу, незвичну, заборонену або високоризикову активність.

Сам факт реєстрації на Платформі не означає, що користувач у всіх випадках зобов'язаний пройти повну KYC-верифікацію, якщо інше не передбачено інтерфейсом, умовами конкретного сервісу або застосовними вимогами.

5.7. Дані служби підтримки:

- контактні дані;
- зміст звернення;
- вкладення, скріншоти, документи та повідомлення;
- історія листування;
- записи звернень, якщо відповідний канал зв'язку передбачає запис;
- відомості про вирішення звернення;
- дані, необхідні для підтвердження володіння акаунтом.

5.8. Маркетингові та комунікаційні дані:

- згоди та відмови від розсилок;
- email, Telegram username, Telegram ID або інший канал зв'язку;
- історія сповіщень;
- уподобання щодо мови та типу повідомлень;
- статистика доставки та взаємодії з повідомленнями, якщо це застосовно.

Ми можемо надсилати сервісні, інформаційні та маркетингові повідомлення, пов'язані з Платформою, безпекою, оновленнями, новими функціями, змінами умов, акціями або іншими пропозиціями Компанії. Ми не прагнемо надсилати користувачу надмірні, такі, що вводять в оману, або нав'язливі повідомлення. Користувач може відмовитися від маркетингових розсилок, якщо така відмова передбачена застосовним законодавством або інтерфейсом Платформи. Сервісні та юридично значущі повідомлення можуть надсилатися незалежно від відмови від

маркетингових повідомлень.

6. Цілі обробки персональних даних

Ми можемо обробляти персональні дані для:

- реєстрації та управління акаунтом;
- авторизації, автентифікації та відновлення доступу;
- надання гарантії та операцій із цифровими активами;
- обробки депозитів, виведень, внутрішніх переказів, балансів, комісій і підтверджень;
- надання P2P-функцій, створення оферів, відкриття та завершення угод;
- резервування, утримання або вивільнення цифрових активів;
- обміну повідомленнями та доказами між учасниками угоди;
- вирішення спорів та арбітражу;
- фіксації платіжного методу та перевірки підтверджень оплати у P2P-спорах;
- AML/KYC/CTF, санкційного контролю та управління ризиками;
- моніторингу транзакцій і перевірки блокчейн-адрес;
- безпеки, запобігання шахрайству, мультиакаунтингу, спаму, фішингу, атакам та іншим порушенням;
- підтримки користувачів;
- покращення Платформи, виправлення помилок, тестування функцій та аналітики;
- юридичних цілей, врегулювання претензій і захисту прав Компанії.

7. Cookies та аналогічні технології

Ми можемо використовувати local storage, session storage, технічні ідентифікатори сесії, серверні журнали, власну аналітику, не засновану на cookies, та інші аналогічні технології для авторизації, збереження налаштувань, захисту сесії, запобігання шахрайству, аналітики, діагностики помилок, покращення роботи Платформи та дотримання вимог безпеки.

Якщо в майбутньому Компанія почне використовувати cookies або сторонню cookie-аналітику, така обробка буде відображена в цій Політиці, окремій Політиці cookies або інтерфейсі згоди, якщо цього вимагатиме застосовне законодавство.

8. Автоматизована обробка та профілювання

Ми можемо використовувати автоматизовані та напівавтоматизовані засоби для аналізу технічних подій, транзакцій, AML-ризиків, підозрілої активності, порушень правил, мультиакаунтингу та інших факторів безпеки.

Платформа позиціонується як privacy-first: ми прагнемо мінімізувати збирання

персональних даних, не запитувати ідентифікаційні документи без необхідності та використовувати ризик-орієнтований підхід до перевірок. Privacy-first не означає повну анонімність і не виключає обробку даних, необхідну для безпеки, дотримання закону, AML/KYC/CTF-процедур, вирішення спорів, запобігання шахрайству та захисту Платформи.

Така обробка може впливати на доступність окремих функцій Платформи, ліміти, необхідність додаткової перевірки, призупинення операції або передання справи на ручну перевірку.

9. Передання даних третім особам

Ми не продаємо персональні дані користувачів і не передаємо їх третім особам для самостійного маркетингу таких третіх осіб без згоди користувача.

Ми можемо передавати персональні дані таким категоріям отримувачів:

1. постачальникам інфраструктури;
2. постачальникам AML/KYC/CTF-сервісів;
3. банкам, платіжним провайдерам і процесингам, лише якщо такі особи беруть участь у конкретному сервісі або операції;
4. постачальникам аналітики та діагностики;
5. постачальникам комунікацій;
6. юридичним, аудиторським і комплаєнс-консультантам;
7. пов'язаним особам Компанії;
8. компетентним органам;
9. контрагентам за P2P-угодою — лише в обсязі, необхідному для виконання угоди;
10. потенційним або фактичним правонаступникам у разі корпоративних змін.

У звичайній P2P-угоді фіатний платіж здійснюється безпосередньо між користувачами, і Компанія не обробляє фіатний платіж як платіжний посередник.

10. Транскордонне передання даних

Платформа може використовувати інфраструктуру, партнерів, підрядників та обробників, розташованих у різних країнах. У зв'язку з цим персональні дані можуть передаватися, зберігатися та оброблятися за межами країни проживання користувача або країни реєстрації Компанії.

Під час транскордонного передання даних ми вживаємо розумних заходів для забезпечення належного рівня захисту персональних даних, включно з договірними зобов'язаннями щодо конфіденційності, технічними та організаційними заходами безпеки, перевіркою постачальників та іншими механізмами, передбаченими застосовним законодавством.

11. Зберігання персональних даних

Ми зберігаємо персональні дані стільки, скільки необхідно для цілей, для яких вони були зібрані, а також для дотримання юридичних обов'язків, вирішення спорів, запобігання шахрайству, захисту прав Компанії та користувачів.

Орієнтовні строки зберігання:

1. дані акаунта — протягом строку існування акаунта та розумного періоду після його закриття;
2. дані транзакцій, балансів, депозитів, виведень і P2P-угод — не менше строку, що вимагається застосовним законодавством, AML/CTF-правилами, бухгалтерськими вимогами або внутрішніми правилами управління ризиками;
3. AML/KYC/CTF-дані — протягом строку, встановленого застосовним законодавством;
4. дані підтримки — протягом строку, необхідного для обробки звернення, вирішення спору, покращення сервісу та захисту прав Компанії;
5. технічні журнали та дані безпеки — протягом строку, необхідного для безпеки, діагностики, розслідування інцидентів і запобігання зловживанням;
6. маркетингові дані — до відкликання згоди або відмови від розсилки, якщо більш тривале зберігання не потрібне для підтвердження факту згоди або відмови.

Видалення акаунта або відкликання згоди не завжди означає негайне видалення всіх даних. Ми можемо зберегти дані, якщо це необхідно для виконання закону, AML/KYC/CTF, бухгалтерського обліку, запобігання шахрайству, вирішення спорів, виконання судових або регуляторних вимог чи захисту прав Компанії.

12. Публічні блокчейн-дані

Користувач розуміє, що операції з цифровими активами можуть записуватися в публічні або частково публічні блокчейн-мережі. Компанія не є оператором таких мереж, не контролює їхню роботу та не може видалити, приховати, змінити або обмежити поширення інформації, вже опублікованої в блокчейні.

13. Конфіденційність акаунта та відповідальність користувача

Користувач зобов'язаний самостійно забезпечувати конфіденційність даних доступу до акаунта, включно з паролем web-версії, PIN-кодом Telegram Mini App, кодами 2FA, пристроями, email, Telegram-акаунтом та іншими засобами авторизації.

Користувач не повинен передавати третім особам пароль, PIN-код, одноразові коди, коди 2FA, seed-фразу, приватні ключі, резервні коди, доступ до пристрою або Telegram-акаунта, а також інші дані, що дають змогу отримати доступ до акаунта або цифрових активів.

Компанія не запитує seed-фрази, приватні ключі, повні дані банківських карток, CVV/CVC-коди або паролі від сторонніх сервісів.

14. Дані третіх осіб

Користувач не повинен передавати Компанії персональні дані третіх осіб без законної підстави та згоди таких осіб, якщо така згода потрібна. Якщо користувач передає дані третіх осіб у межах P2P-угоди, звернення до служби підтримки, спору, завантаження документів або іншої взаємодії з Платформою, користувач підтверджує, що має право передати такі дані.

15. Права користувача

Залежно від застосовного законодавства користувач може мати право:

- на доступ до персональних даних;
- на отримання копії даних;
- на виправлення неточних, неповних або застарілих даних;
- на видалення даних;
- на обмеження обробки;
- на заперечення проти обробки;
- на переносимість даних;
- на відкликання згоди;
- на скаргу до компетентного наглядового органу.

Ми можемо відмовити в повному або частковому видаленні даних, якщо зберігання необхідне для дотримання закону, AML/KYC/CTF-зобов'язань, бухгалтерського обліку, запобігання шахрайству, вирішення спорів, виконання договорів або захисту прав Компанії.

16. Безпека персональних даних

Ми застосовуємо розумні технічні та організаційні заходи для захисту персональних даних, включно з шифруванням передання даних, контролем доступу, розмежуванням прав, журналюванням дій, моніторингом підозрілої активності, резервним копіюванням, процедурами реагування на інциденти та внутрішніми правилами інформаційної безпеки.

Попри вжиті заходи, жоден спосіб передання даних через інтернет і жодна система зберігання не є абсолютно безпечними. Користувач повинен дотримуватися заходів безпеки зі свого боку.

17. Діти та неповнолітні

Платформа не призначена для осіб, які не досягли мінімального віку, необхідного для самостійного використання відповідних сервісів у країні проживання користувача.

18. Посилання на сторонні ресурси

Платформа може містити посилання на сторонні сайти, застосунки, гаманці, блокчейн-оглядачі, платіжні сервіси, Telegram-ресурси або інші зовнішні сервіси. Компанія не контролює такі сторонні ресурси та не відповідає за їхню політику конфіденційності, безпеку, зміст або обробку даних.

19. Зміна Політики

Ми можемо періодично змінювати цю Політику, щоб відображати зміни в Платформі, законодавстві, вимогах партнерів, технологіях, ризиках або внутрішніх процесах. Актуальна версія Політики публікується на сайті <https://kashbi.io> або в інтерфейсі Платформи.

20. Зв'язок з нами

З питань цієї Політики, обробки персональних даних, реалізації прав користувача або скарг користувач може звернутися:

- Компанія: F-Tech
- Країна реєстрації: Kazakhstan
- Сайт: <https://kashbi.io>
- Застосунок: KashBi
- Email: legal@kashbi.io
- Telegram: [kashbi_support](#)
- Юридична адреса: 44/1 Al-Farabi Avenue, Apartment 207

21. Мовні версії

Цей документ може бути опублікований різними мовами. Якщо застосовне законодавство вимагає пріоритету певної мовної версії, застосовується така версія. В інших випадках у разі розбіжностей між мовними версіями пріоритет має версія англійською мовою.