

Homeunity Privacy Notice

Уведомление Homeunity о конфиденциальности

Document effective date / Дата вступления документа в силу: 1 September 2026 / 1 сентября 2026 года

This Notice explains how personal data is collected and used for Homeunity Travel Club, HRPT transactions, partner administration and compliance. It applies to customers, prospective customers, partners, representatives and website users. English prevails.

Настоящее Уведомление объясняет обработку персональных данных в Homeunity Travel Club, операциях HRPT, партнёрской программе и комплаенсе. Оно применяется к клиентам, потенциальным клиентам, партнёрам, представителям и пользователям сайта. Английский текст преобладает.

1 Controller and contact / 1 Контролёр и контакты

For the processing purposes that it determines under this Notice, the controller is Fuchs Treuhand AG, a Swiss stock corporation (Aktiengesellschaft), UID CHE-107.253.643, commercial register number CH-100.3.005.984-2, registered office at Morgartenstrasse 3, 6003 Lucerne, Switzerland. Fuchs also acts as fiduciary and payment administrator for the Homeunity program; where it processes data solely on documented instructions for a separately identified controller, the relevant allocation will be disclosed in the applicable interface or notice. Privacy contact: privacy@homeunity.io. Postal requests may be sent to the registered office.

В отношении целей обработки, самостоятельно определяемых по настоящему Уведомлению, контролёром является Fuchs Treuhand AG, швейцарское акционерное общество (Aktiengesellschaft), UID CHE-107.253.643, номер в торговом реестре CH-100.3.005.984-2, адрес: Morgartenstrasse 3, 6003 Люцерн, Швейцария. Fuchs также действует как фидуциарный и платёжный администратор программы Homeunity; если данные обрабатываются исключительно по документированным поручениям отдельно указанного контролёра, соответствующее распределение ролей раскрывается в применимом интерфейсе или уведомлении. Контакт по вопросам конфиденциальности: privacy@homeunity.io. Почтовые обращения направляются по зарегистрированному адресу.

2 Data collected / 2 Собираемые данные

- Identity and contact data, including name, date of birth, nationality, residence, email, telephone, identity document and likeness where required.
- Compliance data, including beneficial ownership, source of funds or wealth, occupation, tax residence, PEP and sanctions results, risk rating and supporting evidence.
- Transaction and wallet data, including wallet address, network, token amount, payment source, transaction identifiers, order, lock and commission records.
- Partner data, including referral relationships, communications, approved content, Q Volume, status, rewards, complaints and audit findings.
- Technical data, including IP address, device, browser, login, cookies, security events and consent preferences.
- Communications and inferences reasonably necessary to answer requests, prevent fraud and comply with law.
- Идентификационные и контактные данные, включая имя, дату рождения, гражданство, место жительства, email, телефон, документ личности и изображение, когда необходимо.
- Комплаенс-данные: бенефициар, происхождение средств или состояния, занятие, налоговое резидентство, PEP и санкционные проверки, риск-рейтинг и доказательства.
- Данные операций и кошелька: адрес, сеть, количество токенов, источник платежа, идентификаторы транзакций, заказ, lock и комиссии.

- Данные партнёра: реферальные связи, коммуникации, материалы, Q Volume, статус, вознаграждения, жалобы и проверки.
- Технические данные: IP, устройство, браузер, входы, cookies, события безопасности и настройки согласий.
- Сообщения и обоснованные выводы для ответа, предотвращения мошенничества и исполнения закона.

3 Purposes and legal grounds / 3 Цели и правовые основания

Purpose / Цель	Ground or justification / Основание или обоснование
Onboarding and contract performance / Допуск и исполнение договора	Steps requested before contract and performance of contract / Преддоговорные действия и исполнение договора
Identity AML sanctions and fraud controls / Идентификация AML санкции и контроль мошенничества	Legal duties, substantial legitimate interests and, where required, consent / Юридические обязанности существенные законные интересы и при необходимости согласие
Orders delivery locks rewards and support / Заказы передача блокировки выплаты и поддержка	Contract performance and legitimate operational interests / Исполнение договора и законные операционные интересы
Security audit and dispute evidence / Безопасность аудит и доказательства спора	Legitimate interests, legal claims and legal duties / Законные интересы требования и юридические обязанности
Service analytics and essential cookies / Аналитика сервиса и необходимые cookies	Legitimate interests; consent where required / Законные интересы; согласие когда требуется
Promotional communications / Рекламные сообщения	Consent or another lawful basis with an effective opt out / Согласие или иное законное основание с эффективным отказом
Regulatory reporting and retention / Регуляторная отчётность и хранение	Applicable legal obligation / Применимая юридическая обязанность

Основания включают преддоговорные действия, исполнение договора, юридические обязанности, существенные законные интересы, защиту требований и согласие там, где оно требуется. Отказ предоставить обязательные KYC-данные может исключить участие.

4 Recipients processors and international transfers / 4 Получатели обработчики и международная передача

Data may be disclosed on a need-to-know basis to identity and sanctions providers, banks and payment providers, blockchain analytics vendors, hosting and security providers, professional advisers, auditors, competent authorities, courts and replacement administrators. Public blockchain information may be visible worldwide and cannot generally be deleted by the controller. Processors must be selected, instructed and monitored. Transfers outside Switzerland or the EEA require an adequacy basis, approved contractual safeguards, another lawful exception or the data subject's valid consent, as applicable.

Данные могут передаваться по необходимости провайдером идентификации и санкционного контроля, банкам и платёжным организациям, блокчейн-аналитике, хостингу и безопасности, консультантам, аудиторам, компетентным органам, судам и правопреемнику администратора. Публичный блокчейн виден глобально и обычно не позволяет контролёру удалить запись. Обработчики выбираются, инструктируются и контролируются. Для передачи за пределы Швейцарии или ЕЭЗ требуется адекватность, договорные гарантии, иное законное исключение либо действительное согласие.

5 Retention / 5 Хранение

Data is kept only as long as required for the stated purpose, contract, security, limitation periods and mandatory AML, accounting, tax or regulatory retention. The operational schedule should specify exact periods by record class; as a working rule, compliance and transaction files are retained for ten years after the relationship ends where the applicable rule requires it, while unsuccessful onboarding files should be deleted earlier unless needed for risk or legal evidence.

Данные хранятся только на срок цели, договора, безопасности, исковой давности и обязательного AML, бухгалтерского, налогового или регуляторного хранения. Внутренний график должен установить точные сроки; рабочее правило — комплаенс- и транзакционные файлы до десяти лет после прекращения отношений, если это требуется, а неуспешные анкеты удаляются раньше, если не нужны для рисков или доказательств.

6 Security and automated review / 6 Безопасность и автоматизированная проверка

Appropriate organisational and technical controls include least-privilege access, multifactor authentication, encryption in transit and at rest where appropriate, logging, secure document exchange, backups, incident response and periodic access review. Risk scoring and screening tools may flag a case, but a materially adverse decision should receive meaningful human review where required by law.

Применяются минимальные права доступа, MFA, уместное шифрование при передаче и хранении, журналы, защищённый обмен документами, резервирование, реагирование на инциденты и периодическая проверка доступа. Автоматические инструменты могут отметить риск, однако существенно неблагоприятное решение должно проходить содержательную проверку человеком, если этого требует закон.

7 Rights and choices / 7 Права и выбор

Subject to applicable law, a person may request information, access, correction, deletion, restriction or objection; withdraw consent prospectively; request data portability where available; and complain to the competent data protection authority. Identity may be verified before acting. Rights may be limited by legal retention, third-party rights, privilege, security and blockchain immutability.

С учётом закона лицо вправе запросить информацию, доступ, исправление, удаление, ограничение или возражение; отозвать согласие на будущее; запросить переносимость, когда применимо; и обратиться в надзорный орган. Перед исполнением проверяется личность. Права могут ограничиваться обязательным хранением, правами третьих лиц, привилегией, безопасностью и неизменяемостью блокчейна.

8 Children updates and complaints / 8

Несовершеннолетние изменения и жалобы

The services are not intended for persons under 18. Material changes will be dated and communicated through the website, account or verified email. Questions should first be sent to the privacy contact. The competent Swiss authority is the Federal Data Protection and Information Commissioner; EU or EEA residents may also have rights before their local authority when the GDPR applies.

Сервисы не предназначены для лиц младше 18 лет. Существенные изменения датируются и сообщаются через сайт, кабинет или подтверждённый email. Вопросы сначала направляются контакту по конфиденциальности. В Швейцарии компетентен Федеральный уполномоченный по защите данных; жители ЕС/ЕЭЗ также могут обращаться к местному органу, когда применим GDPR.