Уведомление о конфиденциальности

HU-P10 · v6.5 · 12.10.2026

1 Кто отвечает за ваши данные

1.1. Fuchs Treuhand AG определяет цели и способы обработки персональных данных при предоставлении услуг Homeunity и выступает контролёром данных в пределах описанной ниже деятельности.

Реквизиты Компании:

Fuchs Treuhand AG
UID: CHE-107.253.643
Регистрационный номер: CH-100.3.005.984-2
Morgartenstrasse 3
6003 Lucerne
Switzerland

Контакт по вопросам персональных данных: **privacy@homeunity.io**.

1.2. Настоящее уведомление распространяется на сайт Homeunity, кабинет, связанные с ними формы и коммуникации, обслуживание участников Travel Club, операции с HRPT, участие в HAFS и партнёрской программе. При отдельном подключении HPOT оно применяется вместе с дополнительной информацией о соответствующей программе.

1.3. Уведомление объясняет, какие данные обрабатываются, зачем они нужны, кому могут передаваться и как воспользоваться своими правами. Оно не является согласием на все перечисленные виды обработки.

Если для конкретной цели требуется согласие, оно запрашивается отдельно.

1.4. Платёжные организации, поставщики бронирований и внешние сервисы входа или сообщений могут самостоятельно определять цели части своей обработки. В этой части применяются их собственные уведомления. Компания отвечает за данные, которые получает и использует для своих целей.

2 Какие данные обрабатываются

2.1. Данные кабинета и контактов. При регистрации и обслуживании кабинета обрабатываются идентификатор пользователя, предоставленное имя, имя пользователя, контактные данные и сведения о привязанных способах входа.

При использовании подключённого сервиса сообщений Компания получает сведения, передаваемые этим сервисом в рамках выбранного способа входа или взаимодействия с ботом.

2.2. Данные договоров и операций. Для оформления и исполнения операций обрабатываются принятые редакции документов, подтверждения согласия и поручений, сведения о заказах, платежах, приобретении HRPT, аллокациях, начислениях, выплатах, возвратах и обращениях.

Записи могут включать дату и время действия, количество токенов, срок блокировки, применённый коэффициент, сумму, валюту, статус и подтверждение исполнения.

2.3. Данные кошелька включают адрес, сеть, подтверждение контроля при необходимости и относящиеся к операции идентификаторы. Записи allocation определяют количество участника, поручения, позицию, ограничения, возврат и исполнителя каждой операции. Fuchs Treuhand AG не требует приватного ключа или фразы восстановления собственного кошелька участника.

2.4. Данные партнёрского участия. Обрабатываются реферальная связь, сведения об атрибуции операций, квалификационных показателях, статусе, расчёте вознаграждений, корректировках и спорах.

Такие записи необходимы для установления того, кому и на каком основании причитается партнёрское вознаграждение.

2.5. Обращения и переписка. Компания получает содержание ваших сообщений, приложенные вами материалы и сведения, необходимые для ответа. Не следует направлять документы личности или чувствительные сведения через обычную форму поддержки, если их отдельно не запросили по предназначенной для этого процедуре.

2.6. Технические данные. При использовании сайта и кабинета могут обрабатываться IP-адрес, сведения о браузере и устройстве, время обращения, события входа, ошибки, действия, существенные для безопасности, и настройки интерфейса.

Объём зависит от используемой функции и соответствующего журнала.

2.7. Данные поездок. При оформлении бронирования могут потребоваться имена путешественников, контакты, даты и маршрут поездки, состав заказа и сведения о специальных потребностях.

Данные о здоровье или необходимой помощи запрашиваются только в объёме, необходимом для соответствующей услуги, и при наличии требуемого правового основания.

3 Проверка личности и сведения KYC

3.1. Документальная проверка личности проводится, когда необходима для выбранной сделки, через специально установленную процедуру. До запроса документов клиент получает инструкции передачи и сведения о методе, получателях и хранении. Это Уведомление не является просьбой прислать документ личности без отдельного запроса.

3.2. После введения документальной проверки могут обрабатываться данные удостоверения личности, адрес проживания, гражданство, сведения о представителе и его полномочиях, бенефициарном владельце, происхождении средств, цели операции и результатах проверок.

Перечень определяется конкретной услугой и необходимостью проверки, а не применяется целиком к каждому пользователю.

3.3. До начала сбора Компания сообщает способ передачи документов, получателей, страны обработки, применимые сроки хранения и необходимую дополнительную информацию.

Основной планируемый канал — защищённая загрузка в специализированной процедуре. Передача документов по рабочей почте допускается исключительно по предварительной инструкции.

3.4. Селфи, видеозапись, сопоставление лица и проверка присутствия не вводятся настоящим уведомлением. До их применения определяются необходимость и правовое основание обработки, а пользователю предоставляется отдельная информация о выбранном способе.

3.5. Доступ к копиям документов личности ограничивается полномочными лицами, которым он необходим для проверки. Реферальное участие, административная помощь или запрос отдельной услуги не предоставляют автоматически доступ ко всему KYC-досье. Биометрическая обработка при её введении требует собственного применимого правового основания и информации.

4 Откуда поступают данные

4.1. Компания получает данные непосредственно от вас при регистрации, вводе сведений, принятии документов, подаче поручений и обращении в поддержку.

4.2. Часть сведений поступает от используемых вами сервисов входа и сообщений, платёжных организаций, поставщиков услуг, представителей и участников, оформляющих операцию для других лиц.

Состав получаемых сведений зависит от соответствующего взаимодействия.

4.3. Для подтверждения операции могут использоваться публичные записи блокчейна. При необходимых проверках также могут использоваться официальные реестры, санкционные перечни и иные законно доступные надёжные источники.

4.4. Если вы предоставляете данные представителя, бенефициарного владельца или другого путешественника, у вас должно быть основание для их передачи. Соответствующему лицу следует предоставить настоящее уведомление и информацию о конкретной услуге.

Это не отменяет самостоятельных обязанностей Компании по информированию.

5 Для чего используются данные

5.1. Обслуживание и исполнение договоров. Данные используются для создания и обслуживания кабинета, обработки заявок, оформления заказов, исполнения поручений, учёта HRPT и аллокаций, расчёта начислений, выплат и возвратов.

Там, где применяется GDPR, основанием служат действия по вашему запросу до заключения договора и исполнение договора.

5.2. Безопасность и предотвращение злоупотреблений. Компания использует необходимые технические и операционные сведения для защиты доступа, выявления несанкционированных действий, проверки целостности учёта и расследования ошибок.

Соответствующий законный интерес состоит в защите пользователей, активов и работоспособности сервиса. Обработка ограничивается необходимым объёмом с учётом прав затрагиваемых лиц.

5.3. Проверки и обязательная отчётность. Сведения используются для установления личности, полномочий и допустимости операции, соблюдения санкций и иных применимых обязанностей.

Основание определяется конкретной проверкой: исполнение установленной законом обязанности либо допустимый законный интерес в предотвращении мошенничества и незаконного использования сервиса. Наличие программы KYC не означает, что любая запрошенная информация автоматически требуется законом.

5.4. Учёт и защита требований. Компания сохраняет необходимые подтверждения для сверки, бухгалтерского и налогового учёта, рассмотрения претензий, предъявления и защиты требований.

Объём и продолжительность такой обработки зависят от соответствующей обязанности или обоснованной необходимости доказательства.

5.5. Коммуникации. Контакты используются для ответов, подтверждений операций, уведомлений о безопасности и существенных изменениях обслуживания.

Рекламные сообщения направляются на основании отдельного согласия либо иного допустимого законом основания с возможностью отказаться от них.

5.6. Отказ предоставить сведения, без которых невозможно оформить или законно исполнить операцию, может препятствовать соответствующей услуге. Необязательные сведения и маркетинговое согласие не должны представляться как обязательное условие только ради их получения.

6 Кому могут передаваться данные

6.1. Внутри Компании и обслуживающей её команды доступ предоставляется с учётом выполняемой функции: поддержка, техническое администрирование, операции, расчёты, комплаенс и рассмотрение споров.

Полномочия на работу с кабинетом не означают неограниченного доступа ко всем документам пользователя.

6.2. Внешние получатели могут включать поставщиков облачного размещения, хранения документов, почты, системных сообщений, средств входа и технической поддержки.

При подключении соответствующей услуги получателями также могут становиться платёжные организации, поставщики бронирований и исполнители проверки личности или санкционного контроля.

6.3. Поставщик, обрабатывающий данные по поручению Fuchs Treuhand AG, получает только необходимое для задачи с соблюдением применимых договорных требований к обработке. Поставщик, самостоятельно определяющий цели, несёт обязанности контролёра в этой части.

6.4. Партнёрам могут предоставляться сведения, необходимые для подтверждения реферальной атрибуции и расчёта вознаграждения. Это не даёт им права получать полные платёжные реквизиты, документы личности или произвольную историю действий участника.

6.5. Данные могут передаваться профессиональным консультантам, аудиторам, судам и компетентным органам в необходимом объёме и при наличии соответствующего основания.

7 Страны хранения и доступа

7.1. Основная база кабинета и серверы приложения размещаются в Бельгии. Ручные резервные копии базы используют регион Европейского союза. Эти сведения относятся к указанным системам и не означают, что все журналы, обращения поддержки или внешние сервисы остаются в Бельгии либо ЕС.

7.2. Личное хранилище проектных документов используется для материалов проекта и шаблонов, а не для хранения персональных данных участников. К нему не относится заявление о корпоративной настройке региона хранения данных участников.

7.3. Корпоративная почта и отправка системных писем используют регион Европейского союза с европейскими центрами сервиса в Нидерландах и Ирландии. Поддержка этих сервисов может включать уполномоченный доступ из Индии в рамках применимых договорных механизмов поставщика.

7.4. Подключённый сервис сообщений самостоятельно определяет обработку в своей системе. В его опубликованных условиях для пользователей, зарегистрировавшихся из ЕЭЗ или Великобритании, описано хранение в Нидерландах и возможная передача компаниям группы на Британских Виргинских островах и в Объединённых Арабских Эмиратах.

Это описание не распространяется автоматически на всех пользователей сервиса сообщений. Компания отдельно отвечает за данные, полученные через кабинет и бот Homeunity.

7.5. Уполномоченная команда может получать доступ из Швейцарии, Сербии, Гонконга, Германии и Испании. Удалённый доступ из другой страны оценивается как трансграничная обработка и не исключается лишь потому, что основная база остаётся в Европе. Необходимые гарантии применяются до доступа или передачи. До начала обработки с привлечением нового получателя или в другой стране затронутому участнику предоставляется информация, требуемая применимым законодательством о данных, и обеспечиваются необходимые гарантии.

7.6. Указанные регионы основной базы, документов и почты не означают, что весь сетевой трафик, метаданные, журналы, средства входа и вспомогательные процессы ограничены теми же территориями.

Сведения о странах и получателях, относящихся к конкретной обработке, можно запросить по адресу **privacy@homeunity.io**.

7.7. Международная передача требует самостоятельного законного основания. В зависимости от получателя и применимого права используются признанная достаточность защиты, надлежащие договорные или иные предусмотренные законом гарантии либо допустимое исключение для конкретной ситуации.

Само ознакомление с уведомлением не заменяет такие условия. Публикация поставщиком стандартных договорных положений также не подтверждает автоматически их применение к любой передаче.

7.8. Информацию о применимых гарантиях и их копию можно запросить у Компании. При предоставлении могут быть закрыты сведения, охраняемые законом, относящиеся к третьим лицам или раскрывающие защищаемые меры безопасности.

8 Сроки хранения и удаление

8.1. Данные сохраняются в течение периода, необходимого для конкретной цели. Единого десятилетнего срока для всех сведений пользователя не устанавливается.

При определении срока учитываются обслуживание договора, незавершённые расчёты, применимые обязанности хранения и необходимость защиты требований.

8.2. Данные профиля и реферальных связей используются в течение обслуживания кабинета и участия в соответствующей программе. После прекращения отношений Компания определяет, какие сведения ещё нужны для расчётов и подтверждения прав, а какие подлежат удалению или обезличиванию.

8.3. Документы операций, начислений и принятия условий могут сохраняться после закрытия кабинета, если это необходимо для обязательного учёта или разрешения требований. Сохраняемые записи не должны использоваться для несвязанных целей только потому, что технически остаются доступными.

8.4. Для обычного облачного журнала применяется настройка хранения 30 дней, для обязательных облачных аудиторских журналов — 400 дней. Сроки относятся к соответствующим журналам, а не автоматически к отдельным экспортам, бухгалтерским записям или доказательствам расследования. Обоснованное сохранение доказательств может требовать отдельного хранения относящихся данных для применимой цели и срока.

8.5. Ручные резервные копии хранятся отдельно от рабочей базы. Удаление рабочей записи не означает её одновременного удаления из каждой резервной копии.

Копии сохраняются только при наличии цели восстановления или иного обоснованного основания. При восстановлении базы ранее исполненные решения об удалении должны применяться повторно.

8.6. Хранение материалов проверки определяется применимой обязанностью учёта, продолжительностью соответствующих отношений и обоснованной потребностью в доказательствах. Конкретный срок или определяющий критерий сообщается с процедурой проверки до сбора. При исключительном получении по почте необходимые материалы переносятся в установленные записи ограниченного доступа, а ненужные рабочие копии удаляются по процедуре.

8.7. Истечение ссылки входа, выход из кабинета и прекращение доступа сами по себе не являются удалением данных.

По запросу об удалении Компания сообщает, какие действия выполнены и какие категории необходимо сохранить, с указанием основания и применимого срока либо критерия его определения.

9 Cookies и сообщения

9.1. Компонент согласия публичного сайта фиксирует выбор в локальном хранилище браузера под ключом hu-consent. Выбранные функции кабинета могут использовать необходимые сессионные средства и защиту. HU-P11 объясняет хранение в браузере и выбор; для необязательной технологии соответствующий интерфейс предоставляет дополнительные сведения до запроса согласия.

9.2. Необязательные аналитические или рекламные технологии не вводятся фактом принятия договорных условий. Если для них требуется согласие, они включаются после отдельного выбора с возможностью последующего отказа.

Информация о конкретной технологии предоставляется при её подключении.

9.3. От рекламных сообщений можно отказаться предусмотренным в сообщении способом или через **privacy@homeunity.io**.

Отказ от рекламы не прекращает необходимые сообщения об операциях, безопасности и исполнении договора.

10 Безопасность и публичный блокчейн

10.1. Для кабинета используются проверка учётной записи, управление сессиями и разграничение доступа. Это не означает, что каждый вход обязательно сопровождается многофакторной аутентификацией.

10.2. Материалы документальной проверки и хранения требуют защиты, соответствующей чувствительности: ограниченного персонального доступа, защищённой передачи, защиты административных аккаунтов и проверки доступа. Компания не представляет обычную почту или публичную форму как защищённое хранилище документов личности. Вопросы безопасности и предполагаемое раскрытие можно сообщить на privacy@homeunity.io без передачи паролей и приватных ключей.

10.3. Публичный блокчейн раскрывает адреса и сведения о транзакциях третьим лицам по всему миру. Если адрес сопоставлен с человеком, связанные записи могут стать персональными данными.

Компания не может удалить запись из публичного блокчейна посредством удаления кабинета. Это не отменяет обязанностей в отношении доступных ей внутренних записей и связей между ними.

10.4. При выявлении нарушения безопасности Компания принимает меры по его оценке и устранению последствий и направляет предусмотренные законом уведомления.

11 Автоматизированная обработка

11.1. Программные средства используются для работы кабинета, обработки статусов, расчётов и технических проверок. Наличие такого средства не означает, что любое решение о правах пользователя принимается полностью автоматически.

11.2. Если вводится исключительно автоматизированное решение, имеющее юридические или сопоставимые существенные последствия, Компания до его применения обеспечивает требуемую законом информацию о логике, значении и последствиях решения.

Предоставляются применимые права на изложение позиции, оспаривание и содержательный пересмотр человеком.

11.3. Пересмотр проводится уполномоченным лицом, способным оценить обстоятельства и изменить ошибочный результат. Запрос можно направить по адресу **privacy@homeunity.io**.

Ограничения раскрытия, прямо предусмотренные законом, сохраняются.

12 Ваши права и порядок обращения

12.1. В пределах применимого законодательства вы можете запросить информацию об обработке и доступ к своим данным, исправление неточностей, удаление, ограничение обработки или переносимость данных, а также заявить возражение.

Если обработка основана на согласии, его можно отозвать на будущее. Это не отменяет законность обработки до отзыва.

12.2. Запрос направляется на **privacy@homeunity.io** или по почтовому адресу Компании. Укажите сведения, позволяющие найти относящиеся к вам записи, и суть запроса.

Не прикладывайте удостоверение личности без отдельной инструкции. Для защиты ваших данных Компания может запросить соразмерное подтверждение личности или полномочий.

12.3. Компания рассматривает запрос в применимый законный срок. Если допускается продление либо требуется уточнение, вам сообщаются причина и дальнейший порядок.

12.4. Ограничение или отказ возможны только при наличии соответствующего основания, включая обязательное хранение, защиту прав других лиц или установленный законом запрет раскрытия. По возможности предоставляется оставшаяся часть информации.

12.5. Вы вправе обратиться в компетентный надзорный орган или суд без обязательного предварительного обращения к Компании.

В Швейцарии вопросы защиты данных относятся к компетенции Федерального уполномоченного по защите данных и прозрачности — FDPIC. Когда применяется GDPR, также сохраняется право обращения в компетентный орган защиты данных в ЕЭЗ.

13 Несовершеннолетние и изменения уведомления

13.1. Самостоятельная регистрация и участие в программах Homeunity предназначены для лиц от 18 лет. Если в рамках допустимого бронирования предоставляются данные несовершеннолетнего путешественника, они используются только для относящейся к нему услуги и при наличии необходимого основания.

13.2. Существенные изменения обработки отражаются в новой датированной редакции и доводятся через сайт, кабинет или подтверждённый канал связи. Если требуется дополнительное согласие, публикация новой редакции его не заменяет.

13.3. Дополнительное уведомление по отдельной услуге уточняет относящиеся к ней данные, получателей и условия обработки. Оно не отменяет предоставленные законом права.