Privacy notice

HU-P10 · v6.5 · 12.10.2026

1 Responsibility for your data

1.1. Fuchs Treuhand AG determines the purposes and means of processing personal data when providing Homeunity services and acts as data controller within the scope of the activities described below.

Company details:

Fuchs Treuhand AG
UID: CHE-107.253.643
Commercial register number: CH-100.3.005.984-2
Morgartenstrasse 3
6003 Lucerne
Switzerland

Personal data contact: **privacy@homeunity.io**.

1.2. This notice covers the Homeunity website, account interface, related forms and communications, services for Travel Club members, HRPT transactions, HAFS participation and the partner programme. Where HPOT is joined separately, it applies together with additional information about that programme.

1.3. This notice explains what data is processed, why it is needed, to whom it may be disclosed and how to exercise your rights. It is not consent to all the processing described.

Where consent is required for a particular purpose, it is requested separately.

1.4. Payment institutions, booking suppliers and external sign-in or messaging services may independently determine the purposes of some of their processing. Their own notices apply to that processing. The Company is responsible for the data it receives and uses for its own purposes.

2 Data processed

2.1. Account and contact data. Registration and account administration involve processing the user identifier, name supplied, username, contact details and information about linked sign-in methods.

Where a connected messaging service is used, the Company receives the information that service transmits through the selected sign-in method or interaction with the bot.

2.2. Contract and transaction data. To arrange and perform transactions, the Company processes accepted document versions, records of acceptance and instructions, and information about orders, payments, HRPT acquisitions, allocations, accruals, payments out, refunds and enquiries.

Records may include the date and time of an action, token quantity, lock period, coefficient applied, amount, currency, status and evidence of performance.

2.3. Wallet data includes address, network, proof of control where required and relevant transaction identifiers. Allocation records identify the participant's quantity, instructions, position, restrictions, return and the person executing each operation. Fuchs Treuhand AG does not require the private key or recovery phrase of the participant's own wallet.

2.4. Partner participation data. The Company processes referral relationships, transaction attribution, qualification metrics, status, remuneration calculations, adjustments and disputes.

These records are needed to establish who is entitled to partner remuneration and on what basis.

2.5. Enquiries and correspondence. The Company receives the contents of your messages, materials you attach and information needed to respond. Identity documents or sensitive information should not be sent through an ordinary support form unless separately requested through a designated procedure.

2.6. Technical data. Use of the website and account may involve processing IP addresses, browser and device details, access times, sign-in events, errors, actions relevant to security and interface settings.

The scope depends on the function used and the relevant log.

2.7. Travel data. A booking may require travellers' names, contact details, travel dates and itinerary, order details and information about special needs.

Health or assistance information is requested only to the extent necessary for the relevant service and where the required legal basis exists.

3 Identity verification and KYC information

3.1. Documentary identity verification is processed only when required for the selected transaction and through the specifically designated procedure. Before documents are requested, the customer receives the submission instructions and information relevant to the method, recipients and retention. This notice is not a request to send an identity document unsolicited.

3.2. Once documentary verification is introduced, processing may include identity document details, residential address, nationality, representative and authority information, beneficial ownership, source of funds, transaction purpose and verification results.

The required information depends on the particular service and verification needs; the entire list does not apply to every user.

3.3. Before collection begins, the Company explains the submission method, recipients, processing countries, applicable retention periods and other necessary information.

The planned primary channel is secure uploading through a dedicated procedure. Email submission is permitted only exceptionally and following prior instructions.

3.4. Selfies, video recording, facial matching and liveness checks are not introduced by this notice. Before their use, the necessity and legal basis of processing are determined and the user receives separate information about the selected method.

3.5. Access to identity-document copies is limited to authorised persons whose verification duties require it. Referral participation, administrative assistance or a request for a separate service does not automatically grant access to an entire KYC file. Biometric processing, if introduced, requires its own applicable legal basis and information.

4 Sources of data

4.1. The Company receives data directly from you when you register, enter information, accept documents, submit instructions or contact support.

4.2. Some information comes from the sign-in and messaging services you use, payment institutions, service suppliers, representatives and participants arranging a transaction for others.

The information received depends on the relevant interaction.

4.3. Public blockchain records may be used to confirm a transaction. Necessary checks may also use official registers, sanctions lists and other lawfully available reliable sources.

4.4. If you supply data about a representative, beneficial owner or another traveller, you must have a basis for disclosing it. That person should receive this notice and information about the particular service.

This does not remove the Company's own information obligations.

5 Purposes of processing

5.1. Services and contractual performance. Data is used to create and administer accounts, process applications, arrange orders, execute instructions, account for HRPT and allocations, calculate accruals, make payments and provide refunds.

Where the GDPR applies, the basis is taking steps at your request before entering into a contract and performing the contract.

5.2. Security and prevention of misuse. The Company uses necessary technical and operational information to protect access, detect unauthorised actions, verify the integrity of records and investigate errors.

The relevant legitimate interest is protecting users, assets and service operation. Processing is limited to what is necessary, taking account of affected persons' rights.

5.3. Checks and mandatory reporting. Information is used to establish identity, authority and transaction eligibility, comply with sanctions and meet other applicable obligations.

The basis depends on the particular check: compliance with a legal obligation or a permissible legitimate interest in preventing fraud and unlawful use of the service. Having a KYC programme does not mean that every item requested is automatically required by law.

5.4. Records and legal claims. The Company retains necessary evidence for reconciliation, accounting and tax records, complaint handling and establishing or defending claims.

The scope and duration of processing depend on the relevant obligation or justified evidential need.

5.5. Communications. Contact details are used for replies, transaction confirmations, security notices and material service updates.

Marketing messages are sent on the basis of separate consent or another lawful basis, with an option to opt out.

5.6. Declining to provide information needed to arrange or lawfully perform a transaction may prevent the relevant service. Optional information and marketing consent must not be presented as mandatory solely to obtain them.

6 Recipients of data

6.1. Within the Company and the team supporting it, access is granted according to function: support, technical administration, operations, settlements, compliance and dispute handling.

Authority to work with the account interface does not mean unrestricted access to all user documents.

6.2. External recipients may include providers of cloud hosting, document storage, email, system messages, sign-in tools and technical support.

When the relevant service is enabled, recipients may also include payment institutions, booking suppliers and identity verification or sanctions screening providers.

6.3. A provider processing data on Fuchs Treuhand AG's behalf receives only what is needed for the task, subject to applicable contractual processing requirements. A provider determining its own purposes has the responsibilities of a controller for that processing.

6.4. Partners may receive information needed to confirm referral attribution and calculate remuneration. This does not entitle them to full payment details, identity documents or unrestricted participant activity histories.

6.5. Data may be disclosed to professional advisers, auditors, courts and competent authorities to the extent necessary and on an appropriate basis.

7 Storage and access countries

7.1. The primary account database and application servers use hosting in Belgium. Manual database backups use a European Union region. These locations concern the identified systems and are not a representation that every log, support interaction or external service remains within Belgium or the EU.

7.2. The personal project-document repository is used for project materials and templates, not for storing participants' personal data. No corporate participant-data storage-region setting is asserted for that repository.

7.3. Corporate email and system email delivery use the European Union region, with European service centres in the Netherlands and Ireland. Support for these services may include authorised access from India under the provider's applicable contractual mechanisms.

7.4. The connected messaging service independently determines processing within its own system. Its published terms describe storage in the Netherlands for users who registered from the EEA or the United Kingdom, and possible transfers to group companies in the British Virgin Islands and the United Arab Emirates.

This description does not automatically apply to every user of that messaging service. The Company is separately responsible for data received through the Homeunity account and bot.

7.5. Authorised team access may take place from Switzerland, Serbia, Hong Kong, Germany and Spain. Remote access from another country is assessed as a cross-border processing operation; it is not excluded merely because the primary database remains in Europe. Necessary safeguards must apply before access or transfer occurs. Before processing begins with an additional recipient or in another country, the affected participant receives the information required by applicable data protection law and any required safeguards are established.

7.6. The stated regions for the primary database, documents and email do not mean that all network traffic, metadata, logs, sign-in tools and supporting processes are confined to those territories.

Information about countries and recipients relevant to particular processing can be requested at **privacy@homeunity.io**.

7.7. International transfers require their own lawful basis. Depending on the recipient and applicable law, this may involve recognised adequacy, appropriate contractual or other statutory safeguards, or a permissible exception for a particular situation.

Reading this notice does not replace those conditions. A provider's publication of standard contractual clauses also does not automatically establish their application to every transfer.

7.8. Information about applicable safeguards and a copy of them can be requested from the Company. Legally protected information, third-party information or details disclosing protected security measures may be redacted.

8 Retention and deletion

8.1. Data is retained for the period needed for its particular purpose. There is no single ten-year retention period for all user information.

The retention period takes account of contractual administration, outstanding settlements, applicable retention duties and the need to protect legal claims.

8.2. Profile data and referral relationships are used while the account and relevant programme participation are administered. After the relationship ends, the Company determines which information remains necessary for settlement and evidence of rights, and which should be deleted or anonymised.

8.3. Transaction, accrual and acceptance records may be retained after account closure where needed for mandatory recordkeeping or resolving claims. Retained records must not be used for unrelated purposes merely because they remain technically available.

8.4. The standard cloud log store uses a 30-day retention setting and mandatory cloud audit logs use a 400-day setting. These apply to the corresponding logs, not automatically to separate exports, accounting records or investigation evidence. A justified legal hold may require retaining relevant evidence separately for the applicable purpose and period.

8.5. Manual backups are stored separately from the working database. Deleting a working record does not mean simultaneous deletion from every backup.

Backups are retained only for recovery or another justified purpose. When a database is restored, previously implemented deletion decisions must be reapplied.

8.6. Identity-verification retention is determined by the applicable recordkeeping obligation, duration of the relevant relationship and justified need for evidence. The specific period or determinative criterion is supplied with the verification procedure before collection. Where documents are exceptionally received by email, necessary material is transferred into the designated restricted records and unnecessary working copies are deleted under that procedure.

8.7. Expiry of a sign-in link, signing out and termination of access do not, by themselves, delete data.

In response to an erasure request, the Company explains the actions taken and the categories that must be retained, identifying the basis and applicable period or the criterion used to determine it.

9 Cookies and messages

9.1. The public website's consent component records its choice in local browser storage under hu-consent. Account functions may use necessary session and security tools when selected. HU-P11 explains browser storage and choices; the relevant interface provides additional information for any optional technology before consent is requested.

9.2. Optional analytics or advertising technologies are not enabled merely by accepting contractual terms. Where consent is required, they are enabled following a separate choice, with an option to withdraw it later.

Information about a particular technology is provided when it is introduced.

9.3. You may opt out of marketing messages using the method provided in the message or by contacting **privacy@homeunity.io**.

Opting out of marketing does not stop necessary transaction, security and contractual communications.

10 Security and the public blockchain

10.1. Account verification, session management and access controls are used for the account interface. This does not mean that every sign-in necessarily uses multi-factor authentication.

10.2. Documentary verification and transaction records require safeguards appropriate to their sensitivity, including restricted personal access, secure transmission, administrative account protection and review of access. The Company does not describe ordinary email or a public contact form as a secure identity-document repository. Security enquiries and suspected disclosure may be reported to privacy@homeunity.io without sending passwords or private keys.

10.3. A public blockchain exposes addresses and transaction information to third parties worldwide. If an address is linked to a person, the associated records may become personal data.

The Company cannot delete a public blockchain entry by deleting an account. This does not remove its obligations concerning internal records and links between them that are within its control.

10.4. If a security breach is identified, the Company takes steps to assess it and address its consequences and provides the notifications required by law.

11 Automated processing

11.1. Software tools support account operation, status processing, calculations and technical checks. The existence of such a tool does not mean that every decision affecting a user's rights is made entirely automatically.

11.2. Before introducing a solely automated decision with legal or similarly significant effects, the Company provides the information required by law about its logic, significance and consequences.

Applicable rights to express a view, contest the decision and obtain substantive human review are provided.

11.3. Review is performed by an authorised person capable of assessing the circumstances and changing an erroneous outcome. Requests may be sent to **privacy@homeunity.io**.

Disclosure restrictions expressly required by law remain applicable.

12 Your rights and requests

12.1. Subject to applicable law, you may request information about processing and access to your data, correction of inaccuracies, erasure, restriction of processing or portability, and may object to processing.

Where processing is based on consent, you may withdraw it prospectively. Withdrawal does not affect the lawfulness of earlier processing.

12.2. Requests may be sent to **privacy@homeunity.io** or the Company's postal address. Please provide information enabling the relevant records to be located and explain your request.

Do not attach an identity document without separate instructions. To protect your data, the Company may request proportionate evidence of identity or authority.

12.3. The Company handles requests within the applicable statutory period. Where an extension is permitted or clarification is needed, you are informed of the reason and next steps.

12.4. Restriction or refusal requires an appropriate basis, including mandatory retention, protection of others' rights or a statutory disclosure prohibition. The remaining information is provided where possible.

12.5. You may apply to a competent supervisory authority or court without first being required to contact the Company.

In Switzerland, data protection matters fall within the competence of the Federal Data Protection and Information Commissioner, FDPIC. Where the GDPR applies, the right to complain to a competent data protection authority in the EEA is also preserved.

13 Minors and changes to this notice

13.1. Independent registration and participation in Homeunity programmes are intended for persons aged 18 or over. Where a permitted booking includes information about a minor traveller, it is used only for the relevant service and on a necessary lawful basis.

13.2. Material processing changes are reflected in a new dated version and communicated through the website, account interface or a verified communication channel. Where additional consent is required, publication of a new version does not replace it.

13.3. A supplementary notice for a particular service explains the relevant data, recipients and processing conditions. It does not override statutory rights.