PRIVACY POLICY
OF THE HEAVEN&HELL PLATFORM
version of 12 June 2024

Introduction

This Privacy Policy describes how we, Heaven&Hell Ltd., address: QUIJANO & ASSOCIATES (BVI) LIMITED, Quijano Chambers, P.O. Box 3159, Road Town, Tortola, British Virgin Islands, registered under number 2148381 ("**H&H**", "**we**", "**our**", "**us**") collect and use your personal data in connection with your use of the Platform and the Services.

This Privacy Policy consists of two parts:

- **Privacy Notice** – which describes how we collect and use your personal data;
- **Privacy Notice for EU/EEA Residents** – which supplements the Privacy Notice by providing information on personal data processing required under the General Data Protection Regulation;

We provide the Platform and the Services subject to the Terms. Please read the Terms before accessing or using the Services or the Platform.

Children

The Platform and Services are restricted to persons who are at least 18 years of age. We do not knowingly collect personal data from people who are less than 18 years of age in connection with the Platform or the Services. If you – the User – are below 18 years old, you may not use the Platform or the Services or interact with them.

Definitions

All terms not defined in this Privacy Policy shall have the meaning as defined in the Terms or in the GDPR. The following terms used in this Privacy Policy shall have the meaning set forth below:

- **Applicable Data Protection Law** – any applicable laws, statutes, regulations, orders, regulatory requirements, bylaws, and other similar legal instruments in force from time to time relating to data protection, data security, privacy and/or the collection, use, disclosure and/or processing of personal data, including but not limited to the GDPR.
- **controller**, **processor**, **processing,** and other terms relating to personal data not defined here have the meaning as defined in Article 4 of the GDPR.
- **Data Protection Act** – the British Virgin Islands Data Protection Act 2021 passed in April 2021 and brought into force effective 9 July 2021.
- **DAO** – a decentralized autonomous organization led by web3 community members according to rules established by DAO itself.
- **DLT –** distributed ledger technology.
- **EEA** – European Economic Area.

- **Fractal** – Trust Fractal GmbH, located at Kochhannstraße 6, 10249 Berlin, Germany, provider of a decentralized identity authentication solutions.
- **GDPR** – General Data Protection Regulation 2016/679 of 27 April 2016.
- **H&H** – Heaven&Hell Ltd., address: QUIJANO & ASSOCIATES (BVI) LIMITED, Quijano Chambers, P.O. Box 3159, Road Town, Tortola, British Virgin Islands, registered under number 2148381.
- **ICT Systems** – the ICT Systems as defined in the Terms.
- **personal data** – information about identified or identifiable natural person as defined in Article 4(1) of the GDPR.
- **Platform** – the online platform operated by us through which the Services are provided, available at: link.
- **Privacy Policy** – this Privacy Policy.
- **SAFT** – Simple Agreement for Future Tokens as defined in the Terms.
- **Services** – the Services as defined in the Terms.
- **Terms** – the Terms of Service of the H&H Token Platform available at: link
- **Third Party** – as defined in the Terms**.**
- **Third Party Service** – as defined in the Terms.
- **User** ("**you**", "**your**" etc.) – the User as defined in the Terms.

Changes

The current version of the Privacy Policy has been adopted and is effective as of 12 June 2024.

We may change the Privacy Policy from time to time. For example, we may do this when it is necessary due to changes in the Terms, changes in legal requirements or changes in the way we use your personal information. We may also amend the Privacy Policy to make it clearer, more accessible, and/or easier for you to understand.

You should check the Privacy Policy before using the Platform and/or the Services. If we change the Privacy Policy, we will give you access to previous versions of the Privacy Policy.

1. PRIVACY NOTICE

1.1. Controller

We, H&H, are the controller of your personal data to the extent this Privacy Policy applies. We cooperate with TRANSRAAD DAO.

1.2. Purposes of processing of personal data

We collect and process your personal data in connection with your use of the Platform and the Services. As a rule, we process your personal data to the extent necessary to provide the Services, ensure smooth operation of the Platform, as well as for other legitimate purposes. You can find the description of such purposes and legal grounds for processing in greater detail below.

1.2.1. Analytics

We use your personal data for analytical and statistical purposes.

1.2.2. Business operations

We use your personal data for the technical and administration purposes in connection with the maintenance and development of our business. For example, this includes internal assessments, audits, products and services development or improvement and so on.

1.2.3. CDD/KYC

We use your personal data for CDD and Know-Your-Customer identity verification and checks ("KYC") purposes, i.e. performing customer due diligence checks in connection with your use of the Services. For example, this includes collecting data from you, either by us directly or by our KYC service provider(s), in connection with the KYC to identify and verify Users before entering into SAFT.

1.2.4. Compliance

We use your personal data to ensure compliance with the applicable law. For example, this includes processing of your personal data to comply with consumer protection law. We also process your personal data to comply with the GDPR, for example when you submit your request as regards your privacy rights and for accountability purposes.

1.2.5. Contract performance

We use your personal data to perform contracts we have executed with you. For example, this includes contract subject to the Terms under which we provide the Services.

1.2.6. Cookies

We use your personal data in connection with the use of cookies or similar technologies for purposes described in the Section 1.2. For example, we may use cookies for analytical and statistical purposes (Section 1.2.1). Please consult the Cookie Notice to learn more about cookies and similar technologies.

1.2.7. Legal rights

We may use your personal data, if necessary, to establish and assert claims or to defend against claims.

1.2.8. Marketing

We use your personal data for the communication and marketing purposes. For example, this includes providing you with our notifications, email or other messages containing

commercial information about our brand, products, or services. This also includes processing your personal data for the purpose of promoting our brand, including informing you about activities, events and news concerning us.

1.2.9. Security

We use your personal data to ensure the security of the Platform and our ICT Systems and to manage them. For example, we record some of your personal data in system logs (special computer programs used for storing a chronological record containing information about events and actions related to the ICT Systems used for rendering the Services by us).

1.3. Sources of personal data

We collect your personal data from the following sources:

1.3.1. Your data

We collect your personal data from you in connection with your use of the Platform or the Services. For example, we collect data when you provide us with your e-mail address when you create your account. In the schedule below we listed examples of such data collection.

Description	Data collected
You receive an email with a link to fill in the Google Form.	• Data provided by you in the form (including your email address) • Technical data
You create an account on the Platform.	• Account data (including your email address) • Technical data
You go through KYC platform of Fractal (our service provider).	• KYC data (including your name, surname etc.) • Technical data
You sign and execute SAFT.	• Blockchain data (including data about crypto-assets transfers) • Technical data (including data used for the purpose of e-signing SAFT)

1.3.2. Automatic data collection

We collect your personal data from your devices or software in connection with your use of the Platform or the Services. For example, we may collect information about your device, its operating system or other software, hardware details, web browser settings and so on when you are browsing the Platform. We collect this information also when you visit our Platform without registration.

1.3.3. Blockchain networks

We collect data from blockchain networks in connection with providing the Services. Such information may include personal and/or anonymous data (please consult Section 2.3.7 for more details).

1.3.4. Third Parties

We collect your personal data from third parties in connection with your use of the Platform or the Services. For example, we use Fractal for your identification and verification of your identity and we use Google Forms to receive information from you. Please consult our Cookie Notice for more information.

1.4. Right to request access and correction of personal data

To exercise your right(s) contact us (please consult Section 1.5).

You have a right to demand access to your personal data held by us and to be able to correct that personal data where the personal data is inaccurate, incomplete, misleading, or not up-to-date, except where compliance with a request to such access or correction is refused under the Data Protection Act.

1.5. Contact details

You can contact us with any inquiries or complaints in respect of the personal data by email at: hello@transraad.io or in writing to our address: QUIJANO & ASSOCIATES (BVI) LIMITED, Quijano Chambers, P.O. Box 3159, Road Town, Tortola, British Virgin Islands.

1.6. Class of Third Parties to whom personal data is disclosed

As a rule, we do not share your personal data unless it is necessary. For example, we may share your personal data in connection with the provision of the Services under the Terms. We may disclose your personal data to the following categories of recipients:

- our business partners (including service providers and contractors), such as marketing and advertising services providers, analytical tools providers, payment services providers, data storage providers;
- banks, insurance companies and/or other financial institutions;
- H&H group entities, including our affiliates, subsidiaries and, in the event of a merger, acquisition or reorganisation, the Third Party involved;
- public authorities or other third parties when required by law and subject to statutory conditions and restrictions;
- professional advisors, such as lawyers, accountants, consultants, and tax advisors;
- other third parties if admissible under Applicable Data Protection Law (e.g. with your consent).

We require our partners to keep your data secure and confidential under the terms that ensure level of protection essentially equivalent to that described in this Privacy Notice. Please note that some of them act on our behalf as our processors and some act as independent controllers of your personal data. If they are controllers of your data, relevant privacy policies and terms and conditions of such controllers may apply. We encourage you to consult such documents before using such services. We are not responsible for the privacy policies and practices of Third Parties. Below you can find additional information on selected categories of recipients of your data.

1.6.1. Blockchain network participants

Please note that your use of the blockchain networks in connection with the Services, depending on the blockchain protocol, may result in recording some of your personal data on the blockchain. This means that your personal data could be identified directly, when combined with other data, or when anonymous data is de-anonymized. As a result, third parties may potentially access your personal data.

1.6.2. Our affiliates and subsidiaries

We share your personal data with our affiliates and subsidiaries. All such entities adhere to the same level of personal data protection as described in this Privacy Notice. In addition, in case of a merger, acquisition or reorganization, we may share your personal data with an involved party. We will ensure that such third party is obligated to keep your data secure and confidential under the terms that ensure level of protection essentially equivalent to that described in this Privacy Notice.

1.6.3. Public authorities

We may share your personal data with public authorities where required by law and subject to the statutory conditions and limitations.

1.6.4. KYC service providers

We share your personal data with Fractal in order to carry out the KYC procedure in accordance with the law. More information regarding their processing of your data can be found on Fractal's website at: https://app.fractal.id/documents/id/privacy-policy-v12.pdf.

1.7. Obligatory or voluntary provision of personal data

In some cases, provision of your personal data is mandatory by law or necessary to carry out your request or to perform a contract we have with you. If you don't provide us with your personal data in such situations, we may not be able to carry out your request, perform a contract with you (or enter into it) or comply with the law. In some cases, this may mean that we will terminate the contract or stop our engagement with you. For example, if you do not

provide your personal data necessary for the complaint procedure, we may not be able to handle your complaint.

In other cases, provision of your personal data is voluntary. If you don't provide us with your personal data in such situations, we may not be able to carry out your request or achieve our goal. For example, if you do not share your contact details with us, we may not be able to contact you.

2. PRIVACY NOTICE FOR EU/EEA RESIDENTS

2.1. Your privacy and blockchain

Blockchain network is an application of a distributed ledger technology (DLT). A distributed ledger is an information repository that keeps records of certain actions (e.g. transactions) and that is shared across, and synchronized between, a set of DLT network nodes using a consensus mechanism. Blockchains are governed by their protocols, i.e. set of rules describing how a network operates (e.g. how a consensus is reached as regards validating a transaction). Such blockchains are intended to immutably record transactions across a wide network of computers and computer systems. Public blockchains are networks that are publicly accessible. Many blockchain networks are decentralized which means that we do not control or operate them.

When you use the Platform and Services, some of your data may be recorded on public blockchain networks, depending on the Service and the blockchain protocol. This means that your personal data could be determined directly, when combined with other data, or when anonymous data is de-anonymized. As a result, third parties may potentially access your personal data. For example, many public blockchain networks are open to forensic analysis or other blockchain analytics operations which can lead to the unintentional disclosure of your personal data such as financial data or information about your transactions.

This is due to the way blockchain technology works, where transparency and immutability of the data stored on the chain is one of the fundamental principles of the technology. Because blockchain networks are decentralized, we (or our affiliates) are not able to delete or change your personal data from such blockchain networks. Please consult relevant information about the potential risks associated with using blockchain technology set out in the Terms.

2.2. Categories of personal data

We use your personal data only when it is lawful under the Applicable Data Protection Law and only to the extent it is necessary to achieve our purposes (please consult Section 1.5). We collect and use the following types of your personal data in connection with your use of the Platform and the Services.

2.2.1. Account data

The account data includes data collected and used in connection with your account, as well as other basic data, including your contact details. For example, this may include public address of your wallet; email, other information provided by the User (i.a. Discord, Telegram username or other details of social accounts).

2.2.2. Blockchain data

The blockchain data includes anonymous data and, in some cases, your personal data that we receive in connection with your use of the Platform, as well as our activity and the activity of Third Parties connected with operation of the Platform. For example, this includes publicly accessible on-chain information (which can be personal data) and limited off-chain information of technical nature, such as a type of a device, browser version and so on (anonymous data, as a rule). This also includes wallet address which is a personal data when the wallet belongs to you, the User. In general, if blockchain data allows for your identification we treat it as personal data in compliance with the GDPR and Applicable Data Protection Law.

2.2.3. Customer support data

The customer support data includes data collected and used in connection with customer support provided by us to you. For example, this may include your communication with us as regards your rights as a consumer, including by telephone or other means of communication, your participation in our surveys or questionnaires or your other requests, questions, and queries.

2.2.4. CDD/KYC data

The CDD/KYC data includes your personal data processed by us or by our KYC service provider(s) acting on our behalf as well as the results of subsequent processing of such data by us in connection with the KYC. For example, this may include information whether you have passed the KYC, aggregated KYC reports with summary information, information whether you are listed on one of the sanction lists, our decisions as regards you in the context of the KYC and so on. This also includes personal data obtained by our KYC service providers or by us from relevant publicly accessible sources, such as public registers, sanction lists or lists of persons entrusted with prominent public functions (so-called "politically exposed persons").

Please note that in certain cases our KYC service providers are independent data controllers. For example, if you enter into agreement with Fractal, your use of its services is subject to the privacy policies and terms and conditions of that company. We encourage you to consult such documents before using such services. We are not responsible for the privacy policies, terms of use and/or practices of such companies where they are independent data controllers.

2.2.5. Technical data

The technical data includes data collected and used in connection with the ICT Systems. For example, this includes your IP address or other online identifiers, information about your operating system or other software used by your device, hardware details, statistics derived from this data and so on. Most of this information is anonymous data. However, in some cases it may be used to identify you, for example in combination with other data. In such cases we treat it as personal data.

2.2.6. Tracking data

The tracking data includes data collected and used in connection with use of cookies and similar technologies, such as pixels, beacons, tags, device IDs, Local Shared Objects or tracking pixels. Please consult our Cookie Notice to learn more about cookies and similar technologies.

2.3. Legal grounds of processing

We collect and process your personal data in connection with your use of the Platform and the Services. As a rule, we process your personal data to the extent necessary to provide the Services, ensure smooth operation of the Platform, as well as for other legitimate purposes. You can find the description of such purposes and legal grounds for processing in greater detail below.

2.3.1. Analytics

The legal ground for such processing is our legitimate interest (Article 6(1)(f) GDPR), which consists of conducting analyses of your activity, as well as of your preferences to improve functionalities and services provided by us. Where required by law, we will only conduct analytical activities with your consent. Where we use cookies for analytical purposes, Section 2.4.5 below applies.

2.3.2. Business operations

The legal ground for processing your personal data is our legitimate interest (Article 6(1)(f) GDPR), which consists of maintaining and developing our business operations and improving our products and services.

2.3.3. CDD/KYC

The legal grounds for the processing of your personal data are:

a) necessity of processing for the performance of the SAFT (Art. 6(1)(b) of the GDPR) – as regards your personal data required to enter into an agreement, such as your name, surname, address etc.; and
b) if applicable, your explicit consent for processing of your biometric data for the purpose of uniquely identifying you by using capturing face and processing of

the biometric identification solutions (Art. 9(2)(a) of the GDPR) – as regards your biometric data; and

c) if applicable, our legal obligation to apply customer due diligence measures for anti-money laundering or counter-terrorist financing purposes (Art. 6(1)(c) GDPR) – as regards categories of personal data we are obligate to process under the applicable law;

d) our legitimate interest (Article 6(1)(f) GDPR), which consists of fraud detection and compliance with industry standards as regards KYC and/or anti-money laundering or counter-terrorist financing – as regards your other personal data not set out in letters a)-c) above.

2.3.4. Compliance

The legal ground for processing is the necessity of processing for compliance with appropriate legal obligation under applicable law to which we are subject (Article 6(1)(c) GDPR).

2.3.5. Contract performance

The legal ground for such processing is the necessity of processing for either taking steps at your request prior to entering into a contract and/or performance of a contract with you (Article 6(1)(b) GDPR). Please consult the Terms for more detailed description of the Services.

2.3.6. Cookies

The legal grounds for processing your personal data are (depending on the type of cookies) your consent (Article 6(1)(a) GDPR) or necessity of processing for performance of a contract with you (Article 6(1)(b) GDPR). Please consult the Cookie Notice to learn more about cookies and similar technologies.

2.3.7. Legal rights

The legal ground for such processing is our legitimate interest (Article 6(1)(f) GDPR), which consists of the protection of our legal rights.

2.3.8. Marketing

The legal ground of the processing is our legitimate interest (Article 6(1)(f) GDPR), which consists of improving our services, communication with the Users, promotion, and marketing. Where required by law, we will be conducting direct marketing activities only with your consent.

2.3.9. Security

The legal ground of the processing is our legitimate interest (Article 6(1)(f) GDPR), which consists of our need to ensure security and safety of our ICT Systems used in connection with the Platform and the Services.

2.4. Data storage

We store your personal data only as long as necessary for the purposes we collected it. This means that the duration of storage depends on the purpose of processing. For example, we store your personal data for the period when we provide you the Services in accordance with the agreement we have entered with you subject to the Terms. We store personal data processed based on legitimate interest(s), our or those of a third party, until you lodge an effective objection to such processing. Similarly, when we process your personal data based on your consent, we store it until you withdraw your consent.

The duration of storage or use of your data may be extended in certain situations. For example, we may store your personal data after you terminate the agreement with us when required by law. We may also continue to store and use the same dataset if we use it for a different purpose and on a different legal basis, if admissible by law. For example, if you terminate the agreement with us, we may continue to use personal data provided by you in connection with your use of the Services when necessary to establish and assert possible claims or to defend against claims (if we have a legitimate interest to do so).

After the end of the period of data storage, we permanently delete or anonymize your personal data.

Please note that use of the blockchain networks in connection with the Services, depending on the blockchain protocol, may result in recording some of your personal data on the blockchain. This means that your personal data could be determined directly, when combined with other data, or when anonymous data is de-anonymized. As a result, third parties may potentially access your personal data. For example, many public blockchain networks are open to forensic analysis or other blockchain analytics operation which can lead to the unintentional disclosure of your personal data or information about your transactions. This is due to the way blockchain technology works, where transparency and immutability of the data stored on the chain is one of the fundamental principles of the technology. Please consult relevant information about the potential risks associated with using blockchain technology set out in the Terms.

2.5. Data transfers

The level of protection for the personal data outside the European Economic Area (EEA) differs from that provided by the EU law. For this reason, we transfer your personal data outside the EEA only when necessary and with an adequate level of protection.

We secure the adequate level of protection primarily by cooperating with processors of the personal data in countries for which there has been a relevant European Commission decision finding an adequate level of protection for the personal data. Alternatively, we may use the standard contractual clauses issued by the European Commission. If you want to learn more about these safeguards, obtain a copy of them or learn where they have been made available, contact us (please consult Section 1.1 above).

2.6. Your rights

To exercise your right(s) contact us (please consult Section 1.1).

Depending on where you live, you may have different privacy rights. If the EU law applies to you, you have the following rights under the GDPR described below.

Please note that it may be technically impossible, depending on a blockchain protocol, to delete or change any information recorded on-chain in a public blockchain network due to the nature of the blockchain technology. Most blockchain networks are decentralized which means that we do not control or operate them. Because of that, we (or our affiliates) are not able to delete or change your personal data from such blockchain networks. Please consult relevant information about the potential risks associated with using blockchain technology set out in the Terms.

2.6.1. Right to access information

You can request from us information about the processing of your personal data. You may also as a rule request from us a free copy of your personal data that we process. Please note that under certain conditions set out by the Applicable Data Protection Law we may charge a fee for such copy.

2.6.2. Right to correct your data

You can request that we rectify your personal data that we use, for example, when it is inaccurate. You can also complete your data if it is incomplete.

2.6.3. Right to be forgotten

You can request that we erase your personal data under certain conditions prescribed by law. However, this is not an absolute right, and it does not apply in certain conditions, for example, when use of your data is necessary for the establishment, exercise, or defence of legal claims by us.

2.6.4. Right to restrict

You can request that we stop processing your personal data, except for storage, under certain conditions prescribed by law. However, this is not an absolute right, and it does

not apply in certain conditions, for example when use of your data is necessary for the protection of the rights of another natural or legal person.

2.6.5. Right to data portability

You can request that some of your personal data is provided to you, or to another controller, in a commonly used and machine-readable format. This right applies where we use your data based on your consent or a contract and if the processing of your data is carried out by automated means.

2.6.6. Right to withdraw consent

You have the right to withdraw your consent to the processing of your personal data. You can do this at any time. If you withdraw consent, we will stop using your personal data where the basis for processing is consent. Withdrawal of consent does not affect the lawfulness of processing your data based on consent before withdrawal. The right to withdraw consent applies only to the extent that your personal data is processed based on consent.

2.6.7. Right to object

You have the right to object to the processing of your personal data based on our or a third party's legitimate interest(s). You can do this at any time. If you raise an objection, we will stop using your personal data where the basis for processing is our legitimate interest. In exceptional circumstances, we may continue to use your data despite your objection. This exception does not apply when you object to the processing of data for direct marketing purposes, i.e., if you object to it, we will stop processing your personal data on this basis.

2.6.8. Right to lodge a complaint

You can lodge a complaint with the supervisory authority dealing with the protection of personal data. You can lodge such complaint with your local data protection authority.

2.7. Automated decision making

We do not make any decisions based solely on automated processing, including profiling, which produce legal effects concerning you or similarly significantly affects you.