Introduction

This Privacy Policy governs privacy of the Users (you, your, customer) of the https://trastra.com Website ("Website") and app served and operated by us, Trastra ("we", "us", "our") and describes what personal data ("Personal data") is collected and how it is used, processed, stored and managed by us, under the applicable legislation, while you use our Website, our Android and IOS mobile apps ("Apps") and services ("Services").
The reference to Trastra means the reference to:

- **Trastra EU, UAB**, a company registered in Lithuania, official registration number 306044056 and having its official registered address at Eišiškių Sodų 18-oji street, 11, Vilnius, Lithuania ("Trastra").

Before getting aware of this Privacy Policy, we advise you to carefully read our User Agreement, Cookies Policy, in order to get comprehensive insight into the terms and rules referred to our Website and our Services use.

If you use our Services, this means that you have read all the mentioned terms and rules. By consenting to use our Services, you expressly agree with this Privacy Policy and expressly consent to and agree with your Personal data processing as stipulated herein.

General Provisions

This Privacy Policy shall be governed by, construed, interpreted, and enforced in accordance with the laws of the European Union. These provisions may be not applicable exclusively in cases where the applicable and governing law prevails or supersedes. If any provision of this Privacy Policy is, or is found to be, inapplicable or unenforceable under the law, that will not affect the applicability or enforceability of the other provisions of this Privacy Policy. If you do not agree with this Privacy policy, you should immediately refrain from using our Website, Apps and/or our Services.

We reserve the right to alter, vary and revise this Privacy Policy, whenever lawfully required or in view of marketing, commercial, technological, whatever upgrade or as we deem necessary, with considering the applicable law. Such revised or updated versions shall apply from the date of publication, unless otherwise expressly stated. By using our Website, Apps and any such revised or updated versions, you agree with and accept the terms of this Privacy Policy regarding the updates. If you disagree with any revision, alteration, or update, you must stop using our Website, Apps and/or our Services.

Personal Data Collection

We may collect and process your Personal data, as follows:

- **Personal Data** – Your e-mail address, first name and last name, date of birth, resident address, postal address, contact phone number, payment account number, trading account details, bank statements, source of funds and wealth;
- **Identification Data** – Identity documents, occupation, employment industry, financial standing;
- **Verification Data** – Personal data which Trastra collects for the purpose of conducting Customer due diligence under applicable anti-money laundering laws, photo, direct video transmission recording;
- **Background Data** – Trastra collects Personal data available in open source;
- **Preference Data** – Preferences, interests, favourites;
- **Payment and Orders Data** – Personal data regarding your fiat, cryptocurrency payment transactions, transactions activity log, billing, payment details and other financial, crypto and settlement details obtained by us when you use our Services, in order to effect and administer your operations; opened, executed, not executed sale/purchase market / limit / stop-loss and other orders details, orders details, history;
- **Device Data** – Domain and host from which you access the Internet, your computer's or other usable device's IP address, web browser type and the operating system software; unique IDs of your devices when you use Android and/or IOS mobile Apps;
- **Usage Data** – We collect your Personal data during your current and for future Website or Apps visits and use, as provided below in the Cookies section. The date and time you access our Website or Apps; The address of the website from which you linked to our Website, Apps when you visit us;
- **Customer Support Data** – communication between Trastra and the Customer (inquiries submitted via the website, email, social media or chat).

Please be noted, that if you directly disclose your Personal data, or sensitive Personal data (such as, among others, racial or ethnic origin, political opinions, religious beliefs, physical or mental health, membership in any organizations, etc.), through public features, this information may be collected and used by other persons.

Personal Data Processing Purposes

For the purposes of the applicable law, we are the "Data Controller" of your personal information and we will securely retain any data submitted by you to us and/or received by us otherwise.

We may use your Personal data, for the following purposes:

- **Contractual Purpose** – to enter into, perform service agreement and deliver our Services properly (which may include disclosure to relevant Third Parties as set forth below);
- **Analytical Purpose** – to provide general statistics regarding use of our Website or Apps;
- **Marketing Purpose** – to send you welcome email following registration procedures; to send you occasionally our Services updates; to contact you for surveys purposes (you do not have to respond to such surveys); for other marketing purpose;
- **Compliance Purpose** – to maintain accuracy of our records; to verify your Personal data for the purpose of managing our customer relationships and observing the Know Your Client (KYC) rules; to comply with legal and regulatory obligations with respect to Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), prevention of criminal activity and lawfully protect our legal interests, make relevant risk assessments and management;
- **Communication Purpose** – to contact the Customer for administrative purposes such as customer service, address technical or legal issues related to the Service provided, or share updates and notifications about the Service.

Sources of obtaining your Personal data

- from you when you visit our Website, Apps, and/or use our Services;
- from you when you enter into an agreement with us;
- from you when you provide your Personal data for identification and KYC purposes;
- from you when you submit any requests, complaints, e-mails, or call us;
- from our clients when they make transfers to you or identify you as assets recipient;
- from financial institutions;
- from registers;
- from our partners, such as identification vendors;
- from other sources.

Security

Trastra will take appropriate legal, organisational, and technical measures to protect Personal data consistent with applicable privacy and data security laws. Security measures shall be applied in order to protect Personal data from involuntary or unauthorised Processing, disclosure or destruction.

Unless we are obliged or permitted by law to do so, and subject to our relevant Third Parties business relationships (our partners, service providers, contractors,

agents, financial institutions, social media, without limitation), we will not disclose your Personal data to any irrelevant Third Parties, for the purpose of security matters.

Personal data security is highly important to us and to protect your Personal data we will organise and take all the necessary and appropriate measures and technologies to safeguard and secure your Personal data collected through Website or Apps.

To use all features and functions of our Website or Apps, you may be required to submit certain Personal data, including password(s). You are responsible for keeping your password(s) confidential and safe.

While we seek to do our utmost to protect your Personal data, you need to keep in mind that transmission of any information over the Internet is not entirely secured and is implemented at your own risk and discretion. We, therefore, cannot ensure the security of your Personal data transmission to our Website or Apps, whenever that is beyond our reasonable control.

You undertake to notify us immediately of any unauthorized access or use of your account or any other breach of security by e-mail: info@trastra.com and we will notify You in case of a Data Breach occurrence which can lead to severe personal health and financial damages.

Our obligations, pursuant to GDPR and other Personal data protection applicable laws and regulations

Your Personal data will be:

- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
- Used lawfully, fairly, and transparently;
- Accurate and kept up to date;
- Relevant to the purposes we have informed you about and limited only to those purposes;
- Maintained only for as long as necessary for the purposes we have informed you about;
- Securely stored and safeguarded against unauthorized or unlawful processing, as well as loss or destruction, using appropriate technical and organizational safeguards.

Legal Grounds for Persona; Data Processing

Trastra is relying on the following legal grounds when Processing Customer's Personal data:

1. Processing is necessary for the ***performance or entry into a contract*** between You and Trastra (GDPR article 6 (1) (b)), Trastra is Processing Personal data for Contractual and Communication Purposes under contract entered into between Trastra and You;
2. Processing is necessary for compliance with a ***legal obligation*** to which Trastra is subject (GDPR article 6 (1) (c)). Trastra is Processing Personal data for Compliance Purpose under legal obligations to which Trastra is subject to;
3. Processing is necessary for the purposes of the ***legitimate interests*** pursued by Trastra (GDPR article 6 (1) (f)). Trastra is Processing Personal data for Analytical or Personalization Purpose under legitimate interest. As part of this, we must maintain and develop our Website, Apps, technical systems and IT-infrastructure, technical and organizational solutions that may also use your Personal data, in order to provide you with adequate Services.
4. Customer has granted a ***consent*** to the Processing of his Personal data (GDPR article 6 (1) (a)). Trastra is Processing Personal data for Marketing Purpose under Customer's consent.

Personal Data Subject Rights

1. **Right to Access** (GDPR, Article 15) – has the right to ask Trastra to provide a copy of User's Personal data which Trastra Process.
2. **Right to Rectification** (GDPR, Article 16) – User has the right to ask Trastra to rectify Personal data in case the data is incorrect or incomplete.
3. **Right to Erasure** (GDPR, Article 17) – Sometimes called Right-to-be-forgotten, User has the right to ask Trastra to erase Personal data, unless Trastra is obliged to continue Processing User's Personal data under law or under a contract between the User and Trastra, or in case Trastra has other lawful grounds for the continued Processing of Personal data.
    - You may amend or remove any portion of your Personal data at any time by using Website interface, Apps or contacting or emailing us at support@trastra.com. Such amendment or removal of certain Personal data may lead to limiting or cessation of your access to Services.
    - Please note that we are legally obligated to save all previous instances of your Personal data in accordance with the Restriction of Processing clause as set below.
1. **Right to Restriction** (GDPR, Article 18) – User has the right to ask Trastra to restrict the Processing of their Personal data in case the data is incorrect or incomplete or in case their Personal data is Processed unlawfully.
    - The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations require us to store your

Personal data for at least 8 years. Upon amendment or removal of your Personal data, it is archived and safekept separately from processed Personal data (i.e. Restriction of Processing rules apply). Such restricted Personal data is processed purely for storing purposes and cannot be accessed automatically or by unauthorised personnel. Restricted data may only be used or restored only in select ways prescribed by law or legal proceeding. Upon expiry of storage term, restricted Personal data is deleted.

- Your Personal data is stored for as long as their storage is required for appropriate purposes for the processing of Personal data, as well as in accordance with the applicable laws. Personal data may be stored in an electronic form and/or in paper format, provided always that your Personal data will be stored securely and protected against unauthorized or unlawful processing and against loss or destruction, using appropriate technical and organizational measures. When assessing the length of the storage of Personal data, we take into account existing regulatory requirements, aspects of contractual performance, your instructions, and our legitimate interests. If your Personal data is no longer needed for the purposes specified, we will delete them or destroy them.

2. **Information Availability** (GDPR, Article 19) – Trastra is obliged and has provided all the information which the Customer has right to receive. This Policy concludes all the information and is available to You on our Website, Apps at any point of time.
3. **Right to Data Portability** (GDPR, Article 20) – User has the right to ask Trastra to provide the User or, in case it is technically feasible, a third party, their Personal data, which the User has provided to Trastra and which is Processed in accordance with User's consent or a contract between the User and Trastra.
4. **Right to Object** (GDPR, Article 21) – User has the right to object to Processing his Personal data in case there is a reason to believe that Trastra has no lawful grounds for Processing the Personal data.
5. **Right to Withdraw Consent for Data Processing** (GDPR, Article 7) – User is entitled to withdraw the consent granted for the Processing of Personal data et any time. Withdrawal does not affect the lawfulness of the Processing conducted before the withdrawal.
6. **Right to File a Complaint** – User has the right to file complaints regarding Processing of their Personal data.
    - User has a right to lodge a complaint with the respective supervisory authority. In case of an EEA User, it is a local Personal data Protection Inspectorate.

Automated Decision-Making Process

Trastra is providing Cryptocurrency related Services for the Customers, residents from the fixed list of jurisdictions could apply to Trastra for Services. Trastra is using automated decision making in the pre-contractual Processing in order to establish sufficiently whether the Customer is eligible to use Trastra's Services.

Automated decision making refers to a decision which is taken solely on the basis of automated Processing of User's Personal data. This means Processing using, for example, software code or an algorithm, which does not require human intervention.

During the onboarding process, the User is being asked for the address and personal ID. The automated decision making is necessary for entering into agreement with Trastra. The automated decision making is used in order to verify and accept or reject the Customer's application to enter into a service agreement with Trastra. Upon rejection, Trastra will inform the User by email about the reasoning for rejection. In addition to Personal data processing for the purposes of client identification and verification, we will use document authenticity verification Services provided by an external vendor during the client onboarding process, including validation of KYC documentation, and information checking in national registers. For potential sanctions and politically exposed person (PEP) matches, as well as negative information in negative media, we shall use the vendor's overnight screening Services.

For the purposes of implementing our legitimate interests within the AML/CTF framework, we may verify information relating to you against credible publicly available information sources, ensure monitoring of your transactions, orders and providing information to supervisory and investigative authorities in the cases provided by legal requirements; and ensure the maintenance of relevant registers.

Transfer of Personal Data to Third Parties

Trastra may transfer your Personal data to third parties such as:

1. legal and regulatory authorities to whom Trastra is obligated to disclose Customer's Personal data under the law;
2. Server hosts, who store Trastra's data, internet/computer software services providers, companies specializing in IT;
3. Identification & Verification Service providers, who help Trastra verify Customers and keep being compliant;
4. Communication Service providers, who help Trastra stay in touch with the Customers and provide necessary support to You;
5. Marketing Service Providers;
6. Banking Service Providers, who help Trastra offer the Service to You;
7. Other third parties – we use or may use facilities of other relevant Third Parties (our partners, service providers, contractors, agents, financial

institutions, social media, without limitation), in order to provide our Services and deal with certain processes necessary for the operation of Website, App. In that regard, such relevant Third Parties will have access to respective Personal data provided by you and/or received by us otherwise.

Your Personal data could be accessed as needed by and shared with our employees, contractors, agents, consultants or our authorized persons who are required to process this Personal data to perform their duties.

We may also be required to share your Personal data with various financial institutions, and/or law enforcement bodies and officials, supervisory authorities/ regulatory bodies, and financial crime investigation services, courts, in order to comply with applicable legislation, prevent fraud, or enforce an agreement we have with you. We may also share your Personal data in order to comply with applicable laws and regulations, to respond to a legal request from law enforcement, and to enforce an agreement we have with you.

On our Website and Apps we include or may include the references or links to the Third Parties websites. External links may be clickable texts, banners, image links to other websites, without limitation. We do not control outbound websites, nor take responsibility for their content, terms of service or any policies. This Privacy Policy governs only specifically this Website and Apps and does not extend to your use of other websites, even those of our partners and Service providers, social media, etc. We, therefore, advise you to review the privacy policy for other websites prior to using them.

Trastra has taken steps to ensure that these data recipients protect the confidentiality and security of Personal data, and to ensure that Personal data is Processed only for the provision of Service and in compliance with applicable law.

Such third parties may be located in countries outside of the European Economic Area ("EEA") whose privacy regulations may differ and which are not in the list of countries with adequate level of data protection published by the European Commission. In those countries the security of the Personal data (inc. protection against misuse, unauthorized access, disclosure, alteration or destruction) may not be ensured as it is secured in the European Union, due to the lack of adequate data protection level.

However, when transferring collected Personal data outside of the EEA, Trastra shall ensure the application of the appropriate safeguards, like the standard contractual clauses and data processing agreements.

Cookies.

Our Website and Apps use Cookies ("Cookies"), small text files saved to your computer or device in order to customize and improve your experience while

visiting and using our Website or App, according to our Cookies Policy. Our Website and Apps use a Cookies choice reservation allowing you to accept/enable or refuse/disable the use and saving of our Cookies on your computer or another usable device.

You can read more about Cookies by visiting our Cookies Policy.

Social Media

We may have official profiles in social media networks. We advise you to verify the authenticity of such profiles before using them. We will never ask for your passwords or personal details in social media networks. When using the social media buttons, you do so at your own risk and discretion.

Downloads

Any downloadable documents, files or media made available on and through our Website or Apps are provided to you at your own risk. While we stick to any measures regarding genuine downloads, we, however, advise you to verify the downloads authenticity, including by antivirus programs. We accept no responsibility for downloads from the Third Parties websites, external websites.

Email and Marketing Messages

Where we informed you and where you agreed, we may use your Personal data to send you notifications about our Services, various profile news, updates regarding our activities by virtue of email newsletters mailing. Email mailings and marketing messages may contain technologies to track your activities. You may subscribe or unsubscribe of such mailing, contacting us by our e-mail or through details provided in that message.

Contact Us

Should you have any questions regarding this Privacy Policy, processing of your Personal data, please contact us at:

Data Protection Officer: hp@trastra.com

Privacy Policy of UAB “Finansinės paslaugos „Contis“

In addition to this Privacy Policy, please also get acquainted with the Privacy Policy of UAB “Finansinės paslaugos „Contis“ which applies to Personal data protection stemmed out from the relations between you and UAB “Finansinės paslaugos „Contis“.