

These providers have limited access only to your information necessary to perform the tasks for which they were contracted for on our behalf and are contractually bound to protect and to use it only for the purposes for which it was disclosed and which are consistent with this Privacy Policy.

Particular third party service providers that support us in providing the 5(,112 Vervice with respect to the IT support and development and technical support are:

CENTROIDA JSC, 46 Akad. Stefan Mladenov Street, Entr. A, Office 15A, Sofia 1700, Bulgaria

CEVIAN SOFTWARE JSC, 46 Akad. Stefan Mladenov Street, Entr. A, Office 15A, Sofia 1700, Bulgaria

3.3. With other institutions that we have contracted to enable us to provide effectively the 5(,112 Vervice to our Users.

3.4. With the other parties to transfer 5(,112 Tokens such as other Users and their service providers.

We may share information with the other participants to your transfers, including other Users you are sending or receiving 5(,112 Tokens from. The information includes Personal Data necessary to facilitate the transfers.

3.5. With other third parties for our legitimate interest or as permitted or required by law:

We may share information about you with other parties for our legitimate interest or as permitted or required by law, including:

- If we need to do so to comply with a law, legal process or regulations;
- To law enforcement authorities or other government officials, or other third parties pursuant to a subpoena, a court order or other legal process or requirement applicable to us;
- If we believe, in our sole discretion, that the disclosure of Personal Data is necessary or appropriate to prevent physical harm or financial loss or in connection with an investigation of suspected or actual illegal activity;
- To protect the vital interests of a person;
- To investigate violations of or enforce a user agreement or other legal terms applicable to any service;
- To protect our property, services and legal rights;
- To facilitate a purchase or sale of all or part of our business;
- In relation to promoting the 5(,112 service to end users by third party business introducers;
- To help assess and manage risk and prevent fraud against us, our clients and fraud involving our website, mobile app or use of our service, including fraud that occurs at or involves our business partners, strategic ventures, or other individuals, and merchants;
- To companies that we plan to merge with or be acquired by; and
- To support our audit, compliance, and corporate governance functions.

With your consent:

We also will share your Personal Data and other information with your consent or direction, including if you authorize an account connection with a third-party account or platform.

In addition, we may provide aggregated statistical data to third-parties, including other businesses and members of the public, about how, when, and why users visit our website and services. This data will not personally identify you or provide information about your use of the 5(,112 Vervice. We do not share your Personal Data with third parties for their marketing purposes without your consent.

3.6. Aggregated Data.

We may also share aggregated information (information about our users that we combine together so that it no longer identifies or references an individual user) and other anonymized information for regulatory compliance, industry and market analysis, demographic profiling, marketing and advertising, and other business purposes.

3.7. Monitoring.

We may monitor or record telephone calls, emails, web chat or other communications with you for regulatory, security, customer services or training purposes.

3.8. Social Media.

We may review and use public comments and opinions made on social networking sites (e.g., Facebook Twitter, Google+, LinkedIn, YouTube, etc.) to better understand our customers and our provision and development of the REINNO service.

3.9. Business Transfers.

If REINNO or any other company that might be involved in providing the REINNO service is involved in any merger, acquisition, reorganization, sale of assets, transfer of portfolio, bankruptcy, or insolvency event, then we may sell, transfer or share some or all of our assets, including your information in connection with such transaction or in contemplation of such transaction (e.g., due diligence). In this event, we will notify you before your personal information is transferred to a different legal person and/or becomes subject to a different privacy policy.

4. YOUR RIGHTS.

You may exercise any of the rights described in this section before the respective Data Controller pursuant to the Legal Agreements by sending an email from your registered e-mail for REINNO service to the respective Company providing the Service to you under the respective Legal Agreement stated below. Please note that we may ask you to verify your identity before taking further action on your request. Please note that upon receipt of your e-mail we shall try our best to provide you with the requested information and resolve your request in reasonable time, subject to all obligations which we or the related companies have under the applicable laws.

4.1. Managing Your Information.

You have the right to obtain the following:

- Confirmation of whether, and where we are processing your Personal Data;
- Information about the purposes of the processing;
- Information about the categories of data being processed;
- Information about the categories of recipients with whom the data may be shared;
- Information about the period for which the data will be stored (or the criteria used to determine that period);
- Information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing;
- Information about the existence of the right to complain to any regulator;
- Where the data was not collected from you, information as to the source of the data; and information about the existence of, and an explanation of the logic involved in, any automated processing;
- Additionally, you may request a copy of the personal data being processed.

4.2. Rectification of Inaccurate or Incomplete Information.

You have the right to ask us to correct inaccurate or incomplete personal information concerning you (and which you cannot update yourself via your online access to your Online account).

4.3. Data Access and Portability.

You have the right to:

- Receive a copy of your Personal Data in a structured, commonly used, machine-readable format that supports re-use;
- Transfer your Personal Data from one controller to another;
- Store your Personal Data for further personal use on a private device; and
- Have your Personal Data transmitted directly between controllers without hindrance.

In some jurisdictions, applicable law may entitle you to request copies of your personal information held by us.

4.4. Data Retention and Erasure.

We generally retain your personal information for as long as is necessary for the performance of the contract between you and us and to comply with our regulatory obligations. If you no longer want us to use your information to provide the REINNO service to you, you can request that we erase your personal information and close your Account, providing your Account is in good standing, not blocked or somehow limited for compliance, risk or regulatory reasons, or due to your outstanding obligation to us, court order, pledge or order by another regulator or other reason which prevents us by law to close your account or terminate the Service. Please note that if you request the erasure of your personal information:

- We may retain some of your personal information as necessary for our legitimate business interests, such as fraud detection and prevention and enhancing security. For example, if we suspend your Account for fraud or safety reasons, we may retain certain information from that Account to prevent that client from opening a new Account in the future. We are also obliged to retain personal data which we have collected for the purposes of complying with the relevant anti-money laundering and anti-terrorism financing for a period as defined under the applicable law;
- We may retain and use your personal information to the extent necessary to comply with our legal obligations.
- Because we maintain the REINNO service to protect against accidental or malicious loss and destruction, residual copies of your personal information may not be removed from our backup systems for a limited period of time.

4.5. Withdrawing Consent and Restriction of Processing.

Where you have provided your consent to the processing of your personal information by us, you may withdraw your consent at any time by changing your Online account settings or by sending a communication to us specifying which consent you are withdrawing. Please note that the withdrawal of your consent does not affect the lawfulness of any processing activities based on such consent before its withdrawal. Additionally, in some jurisdictions, applicable law may give you the right to limit the ways in which we use your personal information, in particular where (i) you contest the accuracy of your personal information; (ii) the processing is unlawful and you oppose the erasure of your personal information; (iii) we no longer need your personal information for the purposes of the processing, but you require the information for the establishment, exercise or defense of legal claims; or (iv) you have objected to the processing and the verification whether our legitimate grounds override your own is pending.

4.6. Objection to Processing.

In some jurisdictions, applicable law may entitle you to require us not to process your personal information for certain specific purposes (including profiling for marketing purposes) where such processing is based on a legitimate interest. If you object to such processing we will no longer process your personal information for these purposes unless we can demonstrate compelling legitimate grounds for such processing or such processing is required for the establishment, exercise or defense of legal claims. Please note that Data Controllers which are regulated financial institutions, such as credit institutions, e-money institutions or similar are obliged under AML laws to make risk profiling of their customers upon opening of the relationship and constantly during the relationship and this is a legitimate reason. In case you do not wish us to process your personal data for certain specific purposes, which are legitimate purposes to us, you shall have to close your account or we may have to stop providing you some or all of the Services, subject to all conditions for the closing of the account, specified above in this Section.

Where your personal information is processed for direct marketing purposes, you may, at any time ask us to cease processing your data for these direct marketing purposes by sending an e-mail to the contact e-mails below.

4.7. Lodging Complaints.

4.7.1. You should in the first place try to resolve the matter by sending an e-mail to the respective Data Controller under this Privacy Policy from your registered e-mail for the Service:

Where the responsible Data Controller (as outlined in the introduction of the Privacy Policy) is specified to be REINNO, you may contact us at:

Mr. Teodor Savov
tsavov@centroida.ai

4.7.2. Competent Regulator. In case you are not satisfied with the reply or resolution of the respective Data Controller, you have the right to lodge complaints about the data processing activities carried out by us before the competent data protection supervisory authorities as described below.

If the Data Controller responsible for the respective data processing, subject to your complaint, REINNO, Estonia you have the right to file a complaint with its lead supervisory authority, the Estonian Data Protection Inspectorate: <http://www.aki.ee/en/inspectorate/staff-and-contacts>

5. OPERATING GLOBALLY.

To facilitate our global operations, we may be required to transfer, store, and process your information with service providers based in Europe, India, Asia Pacific and North and South America. Laws in these countries may differ from the laws applicable to your Country of Residence. For example, information collected within the EEA may be transferred, stored, and processed outside of the EEA for the purposes described in this Data Protection and Confidentiality Policy. Where we transfer

store and process your personal information outside of the EEA we have ensured that appropriate safeguards are in place to ensure an adequate level of data protection.

6. INTERNATIONAL TRANSFERS.

In case personal information is shared with corporate affiliates or third-party service providers outside the EEA in the absence of an adequacy decision, we have – prior to sharing your information with such a corporate affiliate or a third-party service provider – established the necessary means to ensure an adequate level of Data Protection. We will provide further information on the means to ensure an adequate level of Data Protection on request.

7. SECURITY.

We take the responsibility to ensure that your personal information is secure, kept in an encrypted form on servers, collocated in Special data centers. To prevent unauthorized access or disclosure of information we maintain physical, electronic and procedural safeguards that comply with applicable regulations to guard non-public personal information. Once you are logged into your Online account, all internet communication is secured using TLS technology with High-grade security Encryption (2048 bit keys, certified by LetsEncrypt). We restrict access to your personally identifiable information only to employees who need to know that information in order to provide products or services to you.

If you know or have reason to believe that the credentials of your Online account have been lost, stolen, misappropriated, or otherwise compromised or in case of any actual or suspected unauthorized use of your Account, please contact us following the instructions in the Contact Us section below. While we are dedicated to securing our systems and Services, you are responsible for securing and maintaining the privacy of your password(s) and Online account/profile registration information and verifying that the Personal Data we maintain about you is accurate and current.

8. CAN CHILDREN USE OUR SERVICES?

The REINNO Token Investment Service is not designed to individuals under the age of 18. We do not knowingly collect information, including Personal Data, from children or other individuals who are not legally able to use the REINNO Token Investment Service. If we obtain actual knowledge that we have collected Personal Data from an individual under the age of 18, we will promptly delete it, unless we are legally obligated to retain such data. Contact us if you believe that we have mistakenly or unintentionally collected information from an individual under the age of 18.

9. CHANGES TO THIS PRIVACY POLICY

We reserve the right to modify this Privacy Policy at any time in accordance with this provision. If we make changes to this Privacy Policy, we will post the revised Privacy Policy on the Website for the Service. If you disagree with the revised Privacy Policy, you may cancel your Account. If you do not cancel your Account before the date the revised Privacy Policy becomes effective, your continued access to or use of the REINNO Token Investment Service will be subject to the revised Privacy Policy.

10. CONTACT US

If you have any questions or complaints about this Privacy Policy or our information handling practices, you may email us from your Client's email for the Services to the e-mails stated above in **Section 4.7**.