Privacy Policy

We respect the privacy of all users of our website www.coinlio.io and ensure that personal information of the consumers will be treated confidentially. This privacy policy applies to acquisition of LION and the services of the CoinLion platform. We are not responsible for the privacy policy of other websites and sources. By using our website, you indicate that you accept this Privacy Policy.

What is Personal Information and why do we collect it? Personal Information is information or an opinion that identifies an individual. Examples of Personal Information we collect include: names, addresses, email addresses, and phone and facsimile numbers. This Personal Information is obtained in many ways including correspondence, by telephone and facsimile, by email, via our website, from media and publications, from other publicly available sources, and from third parties. We don't guarantee website links or policy of authorized third parties. We collect your Personal Information for the primary purposes of enabling you to use the CoinLion Platform. We may also use your Personal Information for secondary purposes closely related to the primary purpose, in circumstances where you would reasonably expect such use or disclosure. When we collect Personal Information we will, where appropriate and where possible, explain to you why we are collecting the information and how we plan to use it.

Sensitive Information. Sensitive information includes information or opinion about such things as an individual's racial or ethnic origin, political opinions, membership of a political association, religious or philosophical beliefs, membership of a trade union or other professional body, criminal record, or health information. Sensitive information will be used by us (if at all) only:

- For the primary purpose for which it was obtained;
- For a secondary purpose that is directly related to the primary purpose; and
- With your consent or where required or authorized by law.

Third Parties. Where reasonable and practicable to do so, we will collect your Personal Information only from you. However, in some circumstances we may be provided with information by third parties. In such a case we will take reasonable steps to ensure that you are made aware of the information provided to us by the third party.

Disclosure of Personal Information. Your Personal Information may be disclosed in a number of circumstances including the following:

- Third parties where you consent to the use or disclosure; and
- Where required or authorized by law.

Security of Personal Information. Your Personal Information is stored in a manner that reasonably protects it from misuse and loss and from unauthorized access, modification, or disclosure. When your Personal Information is no longer needed for the purpose for which it was obtained, we will take reasonable steps to destroy or permanently de-identify your Personal Information. However, most of the Personal Information is or will be stored in client files which will be kept by us for a minimum of 5 years.

Access to your Personal Information. You may access the Personal Information we hold about you to update or correct it, subject to certain exceptions. If you wish to access your Personal

Information, please contact us in writing. We will not charge any fee for your access request, but may charge an administrative fee for providing a copy of your Personal Information. In order to protect your Personal Information, we may require identification from you before releasing the requested information.

Maintaining the Quality of your Personal Information. It is an important to us that your Personal Information is up to date. We will take reasonable steps to make sure that your Personal Information is accurate, complete, and up-to-date. If you find that the information we have is not up to date or is inaccurate, please advise us as soon as practicable so we can update our records and ensure we can continue to provide quality services to you.

Policy Updates. This Policy may change from time to time and is available on our website.

Privacy Policy Complaints and Inquiries. If you have any questions or complaints about our Privacy Policy, please contact us through the Contact Form on coinlion.io.

Know Your Customer (KYC) & Anti-Money Laundering (AML) Policy

The Company protects itself from involvement in money laundering or suspicious activity by the following:

- Performing an enterprise-wide risk assessment to determine the risk profile of the Company
- Establishing AML policies and procedures
- Implementing internal controls throughout its operations that are designed to mitigate risks of money laundering
- Performing know your customer ("KYC") procedures on all users
- Designating a Compliance Officer with full responsibility for the AML Program
- Conducting an annual AML audit
- Providing AML training to all employees

Policies & Procedures. Prior to launch of the CoinLion Platform, the KYC & AMC Policies will be written and approved by the Company's (Coin Lion, LLC) owners. Once approved, the policies will be provided to all employees. Each employee will acknowledge the Policy in writing. All policies and procedures will be reviewed and updated or revised as needed, but no less often than annually.

Internal Controls. The Company has developed and implemented internal controls to ensure that all of its operations comply with all AML legal requirements and that all required reports are made on a timely basis. Some of those internal controls are listed within this document and include, but are not limited to, the Customer Identification Program, the Suspicious Activity Reporting system, and the required reports on the Program's effectiveness to the Company's Owners.

Training. All officers and employees of the Company are required to receive AML training at least annually. New employees will receive appropriate AML training within 30 days of their hire date. Training for all employees will include not only the legal elements of AML laws and regulations but will also cover job specific applications of these laws. Ongoing training will be provided and updated regularly to reflect current developments and changes to laws and regulations.

Customer Identification. It is the Company's policy to ensure that it has reasonably identified each customer who uses the CoinLion Platform. Users may be identified using a variety of methods.

Account Opening Procedures. When a User opens an account to begin using the CoinLion Platform, the Company will, as part of its account-opening process: (i) cross-check the names of users against compliance databases such as the OFAC Specially Designated Nationals list and other governmental watch lists; (ii) require users to provide proof of identification; and (iii) not permit any payment above 1,000 USD to be made with incomplete account-opening information.

Individual Proof of Identification.

1. Name
2. Date of birth
3. Residence address and mailing address if different (PO Box alone will not be acceptable)
4. Official issued identification number (e.g., passport number, social security number, employee identification number or individual taxpayer identification number)
5. Copy of valid photo identification of the principal(s) involved with the account (e.g., driver's license, passport, alien identification card)

Verification. Documents used in opening an account relationship must be verified prior to establishing the account. Verification of identity will require multi-factor authentication, layered security, and other controls to ensure a meaningful user identity confirmation process based on account size or other factors.

Suspicious Transaction and Activity Reports. The Company will diligently monitor transactions for suspicious activity. Transactions that are unusual will be carefully reviewed to determine if it appears that they make no apparent sense or appear to be for an unlawful purpose. Internal controls will be implemented so that an ongoing monitoring system is in place to detect such activity as it occurs. When such suspicious activity is detected, the Company will determine whether a filing with any law enforcement authority is necessary. Suspicious activity can include more than just suspected money laundering attempts. Activity may be suspicious, and the Company may wish to make a filing with a law enforcement authority, even if no money is lost because of the transaction. The Company will initially make the decision of whether a transaction is potentially suspicious. Once the Company has finished the review of the transaction details, it will consult with the Company's senior management to make the decision as to whether the transaction meets the definition of suspicious transaction or activity and whether any filings with law enforcement authorities should be filed. The Company will maintain a copy of the filing as well as all backup documentation. The fact that a filing has been made is confidential. No one, other than those involved in the investigation and reporting should be told of its existence. In no event should the parties involved in the suspicious activity be told of the filing. The Company may inform the Company's Board of the filing and the underlying transaction.

Reporting Requirements. Reasonable procedures for maintaining records of the information used to verify a person's name, address, and other identifying information are required under this Policy. The following are required steps in the record keeping process:

- The Company is required to maintain a record of identifying information provided by the customer.
- Where the Company relies upon a document to verify identity, the Company must maintain a copy of the document that the Company relied on that clearly evidences the type of document and any identifying information it may contain.
- The Company must also record the methods and result of any additional measures undertaken to verify the identity of the customer.
- The Company must record the resolution of any discrepancy in the identifying information obtained.
- All transaction and identification records will be maintained for a minimum period of five years.

AML Audit. The Company is responsible for directing the annual AML audit of the Company's operations. The independent audit will be conducted by an independent third party with working knowledge of BSA requirements, or by Company personnel with working knowledge of BSA requirements. The Company will develop corrective action plans for all issues that are raised in the audit and will provide the audit report and all corrective action plans to the Company's senior management for review. Reports of the corrective action will continue until all issues are resolved.

Digital Advertising Privacy Information
CoinLion may place cookies on visitors' browsers to collect data (IP address, cookie identifiers, website activity) and analyze traffic on the site. Depending on the browser that you use, you can set your preferences to block/ refuse cookies, and/ or notify you before they are placed.