CoinAnalyst UG (haftungsbeschränkt) („**CoinAnalyst**“) aims to ensure the integrity of its ecosystem. An integral part of the mechanisms to ensure this integrity are measures to combat usage of CoinAnalysts products, especially the CoinAnalyst token (“**COY**”) issued during the Initial Coin Offering (“**ICO**”), for money laundering or terrorist financing (“**AML**”).

CoinAnalyst is not mandatorily obliged by law to apply AML-measures since it does not fall within the scope of the obliged entities as defined in Sec. 2 para. 1 GwG. Due to this the provisions of the GwG will not be directly applicable but will be used correspondingly to the extent that such corresponding application does not violate statutory law. CoinAnalyst obliges itself to apply AML-measures during the ICO on all purchase agreements on voluntary basis. The customer will be requested to consent in processing its data to apply AML measures.

This Anti Money Laundering and Terrorist Financing policy (“**AML policy**”) defines the rules and procedures to prevent usage of the COY for AML purposes.

1. KYC-principles

The basis of CoinAnalyst’s AML measures is the application of the know your customer-principle (“**KYC**” principle) as presupposed i.e. in Sec. 10 et. seq. German Anti Money Laundering Act (*Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten*, *GwG*).

CoinAnalyst will apply the following KYC-measures during the ICO:

1.1 KYC-measures

In general CoinAnalyst will apply the general due diligence obligations (*Allgemeine Sorgfaltspflichten*) within the meaning of Sec. 10 GwG. Therefore CoinAnalyst will:

- identify the customer,
- verify the identity of the customer,
- assess, whether the customer is acting for its own account or for a differing beneficial owner and – in the latter case – the identification of the beneficial owner,

- assess, whether the customer is a political exposed person ("**PEP**"), a family member of a PEP or a known close affiliate, and

- monitor the transactions.

(a) Identification and verification of the customer's identity

The identification of the customer is performed in accordance with Sec. 11 GwG. Within the purchase process the customer is required to provide CoinAnalyst with the following information:

Natural person:	Legal person:
• Pre- and surname,	• Company name,
• Place of birth,	• Legal form,
• Date of birth,	• Registration number (if applicable),
• Nationality, and	• Commercial seat or address, and
• Residential address.	• Names of the members of the management body or names of the legal representatives and – as far as a such a person is a legal person – the aforementioned data on this person.

(b) Verification of the information

The information provided by the customer will be verified in accordance with Sec. 12 para. 1, 2 GwG (*Identitätsprüfung*). The verification will be based on a valid official passport or identity card of the customer which includes a picture of the customer.

The verification of the information will be generally outsourced to a specialized service provider which is acknowledged by the competent authorities. As such CoinAnalyst for the ICO plans to enter into a business relationship with IDnow GmbH.

For future token sales after the ICO, CoinAnalyst can allow verification of the data by equally secure, officially approved procedures.

(c) Assessment of the actions for a deviating beneficial owner

In case of natural persons as customers CoinAnalyst expects the customer to act for its own account. A deviating beneficial owner is therefore excluded.

In case of legal persons CoinAnalyst will examine the ultimate beneficial owner ("**UBO**") in accordance with Sec. 3 GwG. CoinAnalyst will therefore require the customer to submit information on the corporate structure until a sufficient overview on the corporate structure is possible. The submitted information will be supplemented by publicly available as well as by information acquired by third party service providers (such as Thomson Reuters).

(d) Assessment of the PEP-status

CoinAnalyst will assess whether the customer meets the definition of a "Politically Exposed Person", a relative of a PEP or a known close affiliate (as defined in Sec. 1 para. 12-14 GwG) by self-disclosure of the customer. In the purchase process the customer will be informed on the definition of a PEP, a family member of aPEP or a known close affiliate. Afterwards the customer is required to declare whether he meets the definition. In case the customer declare to be a PEP, a family member or a known close affiliate, CoinAnalyst will decide on a case-by-case basis if it either applies enhanced customer due diligence obligations (within the meaning of Sec. 15 GwG) or decides to reject the customer's offer to purchase COY.

(e) Transaction monitoring

CoinAnalyst will monitor in house the transactions during the token sale on suspicious transactions which may be connected with AML. Especially CoinAnalyst will ensure to implement adequate measures to avoid customers bypassing thresholds by way of "smurfing". That means CoinAnalyst will implement measures to identify multiple purchases with a small amount that intend to avoid the reach of an amount that would be otherwise subject to an increased assessment by CoinAnalyst.

CoinAnalyst may decide to use third party solutions or outsource the transaction monitoring.

1.2 Application of simplified or enhanced due diligence measures

In case of transactions with a volume less than EUR 1000,00 or a respective amount in another accepted currency (as defined in Clause 6.3 of the Initial Token Sale Terms and Conditions) CoinAnalyst expects that such transactions will have only a lower risk to be used for money laundering or terrorist financing. Therefore CoinAnalyst decided to apply simplified due diligence obligations (within the meaning of Sec. 14 GwG) on such transactions. If the prerequisites of simplified due diligence are given CoinAnalyst will waive the verification of the customer identity.

The application of simplified due diligence measures is excluded in case that enhanced due diligence obligations need to be applied, mainly in case the customer meets the definition of a PEP. Further enhanced due diligence obligations are applied in case of suspicious transactions especially in case of smurfing. Secondly, CoinAnalyst will apply general due diligence obligations also on customers purchasing COY below an amount of the threshold of EUR 1000,00 on basis of a random sample. The random sample will include an amount up to 5 % of the customers in the ICO. The relevant customers will be informed that they have to verify their identity via IDnow before the purchase offer may be accepted.

2. Measures in case of suspicious transactions

In case CoinAnalyst discovers suspicious transactions which bear the risk for money laundering or terrorist financing CoinAnalyst will firstly examine the relevant transactions in more depth. In such case CoinAnalyst may require the customer to submit further information on the transaction. Such information may be *inter alia*:

- information on the source of the funds, and/ or

- details on the background of the customer (e.g. occupation).

In case CoinAnalyst cannot sufficiently exclude the risk that the transaction is used for money laundering or terrorist financing CoinAnalyst will reject the customer’s offer. In case the purchase agreement is already concluded CoinAnalyst will evaluate whether the purchase agreement may be terminated. In case CoinAnalyst sees significant evidence indicating that a transaction might be connected with money laundering or terrorist financing CoinAnalyst will inform the competent authorities.

3. Record keeping

CoinAnalyst will store the information collected for AML purposes up to five years beginning with the conclusion of the business relationship. In case of ongoing investigation proceedings the storage period may be extended.

4. Amendments

CoinAnalyst will review the AML policy periodically and may amend the AML policy from time to time in its sole discretion and without prior notice.