

Internal AML / CFT / CPF Policy

BYTERIVERS N.V.

Introduction

<https://betsolutions.com/> is operated by **BYTERIVERS N.V.**, a company registered in Curacao with company registration number 164516, with a registered address at Kaya W.F.G. (Jombi) Mensing 24 Unit A, Curaçao (“Company”, “We”).

It is the policy of the Company to prohibit and actively prevent money laundering, the financing of proliferation, and any activity that facilitates money laundering or the funding of terrorist or criminal activities. The Company strives to comply with all applicable requirements under the legislations in force in the jurisdictions in which the Company operates, to prevent the use of the financial system for the purpose of money laundering and terrorist financing.

The Company is accredited and regulated by Curacao Gaming Authority (CGA) to offer accredited services, and namely making available, provision, sale, rental of software and hardware related to games of chance through whatever form or structure over the internet, under the National Ordinance on Games of Chance (Landsverordening op de Kansspelen – LOK). Under the license conditions issued by Curaçao, the Company is required to have in place adequate measures to prevent its systems from being used for the purposes of money laundering, proliferation financing, terrorist financing or any other criminal activity.

The objective of the AML Policy: We seek to offer the highest security to all of our partners and clients on <https://betsolutions.com/>; for that, partner’s or/and client’s (Counterparties) verification is done to ensure the identity of our Counterparties. The reason behind this is to prove that the details are correct and the Counterparty with which Company concludes contract relations is trustworthy and uses not steal information or be used by someone else, which is to create the general framework for the fight against money laundering. We also take into the accord that different safety measures must be accepted depending on the nationality and origin and the way of payment.

<https://betsolutions.com/> also puts reasonable measures to control and limit ML risk, including dedicating the appropriate means.

<https://betsolutions.com/> is committed to high standards of anti-money laundering (AML) according to the Curaçao and EU guidelines and compliance and requires management & employees to enforce these standards in preventing the use of its services for money laundering purposes.

Definition of money laundering

Money Laundering is understood as:

- The conversion or transfer of property, especially money, knowing that such property is derived from criminal activity or from taking part in such activity, to conceal or disguise the illegal origin of the property, or helping any person who is involved in the commission of such an activity to evade the legal consequences of that people or companies action;
- The concealment or disguise of the true nature, source, location, disposition, movement, and rights concerning, or ownership of, property, knowing that such property is derived from criminal activity or an act of participation in such activity;

- The acquisition, possession, or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from assisting in such activity;
- Participation in, association to commit, attempts to commit and to aid, to abet, facilitate, and to counsel the commission of any of the actions referred to in points before.

Money laundering shall be regarded as such even when the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

Proliferation financing (PF) is the provision of funds or financial services for the manufacture, acquisition, possession, development, export, trans-shipment, or use of nuclear, chemical, or biological weapons and their means of delivery.

Organization of the AML for <https://betsolutions.com/>

Following the AML legislation, <https://betsolutions.com/> has appointed the “highest level” for preventing ML: The entire management of **BYTERIVERS N.V.** is in charge. The management is responsible for the formal approval of the business risk assessment (BRA) and ensuring it is reassessed at least annually.

Furthermore, an AMLCO (Anti Money Laundering Compliance Officer) is in charge of enforcing the AML policy and procedures within the System.

The AMLCO is placed under the direct responsibility of the general management.

AML policy changes and implementation requirements

Each significant change of <https://betsolutions.com/> AML policy is subject to approval by the general management of **BYTERIVERS N.V.** and the Anti-money laundering compliance officer.

Verification

Each Counterparty must go through the verification process to work with **BYTERIVERS N.V.** The data and information that are collected before the establishment of the Business Relationship, with the aim of constructing the Counterparty’s economic profile and, as a minimum, shall include the following:

- the purpose and the reason for requesting the establishment of a Business Relationship;
- the anticipated account turnover, the nature of the transactions, the expected origin of incoming funds to be credited in the account and the expected destination of outgoing transfers/payments;
- the Counterparty’s size of wealth and annual income and the clear description of the main business/professional activities/operations.

(the data and information that are used for the construction of the Counterparty's-legal person's economic profile shall include, inter alia, the following:

- the name of the company;
- the country of its incorporation;
- the head offices address;
- the names and the identification information of all natural persons holding 25% or more of shares or voting rights;
- the names and the identification information of the directors;
- the names and the identification information of the authorized signatories;
- financial information;
- the ownership structure of the group that the Counterparty's-legal person may be a part of (country of incorporation of the parent company, subsidiary companies and associate companies, main activities and financial information).

For the verification of the identity of the legal person, the Company shall request and obtain, among others, original or certified true copies of the following documents:

1. certificate of incorporation and certificate of good standing (where available) of the legal person;
2. certificate of registered office;
3. certificate of directors and secretary;
4. certificate of registered shareholders in the case of private companies and public companies;
5. memorandum and articles of association of the legal person;
6. in the cases where the registered shareholders act as nominees of the Beneficial Owners, a copy of the trust deed/agreement concluded between the nominee shareholder and the Beneficial Owner, by virtue of which the registration of the shares on the nominee shareholder's name on behalf of the Beneficial Owner has been agreed;
7. documents and data for the verification of the identity of the persons that are authorized by the legal person to operate the account, as well as the registered shareholders and Beneficial Owners of the legal person.

Where deemed necessary for a better understanding of the activities, sources and uses of funds/assets of a legal person, the Company shall obtain copies of its latest audited financial statements (if available), and/or copies of its latest management accounts.

As an additional due diligence measure, on a risk-sensitive basis, the Company shall carry out (when deemed necessary) a search and obtain information from the records of the Registrar of Companies and from a corresponding authority in the company's (legal person's) country of incorporation (for foreign companies) and/or request information from other sources in order to establish that the applicant company (legal person) is not, nor is in the process of being dissolved or liquidated or struck off from the registry of the Registrar of Companies and that it continues to be registered as an operating company in the records of the Registrar of Companies or by an appropriate authority in any country.

It is pointed out that, if at any later stage any changes occur in the structure or the ownership status or to any details of the legal person, or any suspicions arise emanating from changes in the nature of the transactions performed by the legal person via its account, then it is imperative that further enquiries should be made for ascertaining the consequences of these changes on the documentation and information held by the Company for the legal person and all additional documentation and information for updating the economic profile of the legal person is collected.

Apart from verifying the identity of the Beneficial Owners, the Company shall identify the persons who have the ultimate control over the legal person's business and assets. In the cases that the ultimate control rests with the persons who have the power to manage the funds, accounts or dealing in securities of the legal person without requiring authorization and who would be in a position to override the internal procedures of the legal person, the Company, shall verify the identity of the natural persons who exercise ultimate control as described above even if those persons have no direct or indirect interest or an interest of less than 10% in the legal person's ordinary share capital or voting rights.

Risk management

To deal with the different risks and different states of wealth in other regions on the earth <https://betsolutions.com/> will categorize every nation into three distinct regions of risk.

Targeted financial sanctions

The company shall screen all counterparties against the UN sanctions list (<https://main.un.org/securitycouncil/>) and EU sanctions list (<http://www.sanctionsmap.eu/>). All natural and legal persons in Curaçao are required to freeze without delay and without prior notice the funds or assets of designated persons.

Low Risk Counterparties

The Company shall accept Counterparties which are categorized as low risk as long as the general principles of this Manual are followed.

Moreover, the Company shall follow the Simplified Counterparty Identification and Due Diligence Procedures for low risk Counterparties.

Normal Risk Counterparties

The Company shall accept Counterparties who are categorized as normal risk Counterparties as long as the general principles of the Manual are followed.

High Risk Counterparties

The Company shall accept Counterparties who are categorized as high risk Counterparties as long as the general principles of the Manual are followed.

Moreover, the Company shall apply the Enhanced Counterparty Identification and Due Diligence measures for high risk Counterparties and the due diligence and identification procedures for the specific types of high risk Counterparties mentioned as well as applicable.

Not Acceptable Counterparties

The following list predetermines the type of Counterparties who are not acceptable for establishing a Business Relationship or an execution of an Occasional Transaction with the Company:

- US residents;
- Shell banks or entities subject to targeted financial sanctions;
- Counterparties which fail or refuse to submit, the requisite data and information for the compliance;
- Counterparties whose own shares or those of their parent companies (if any) have been issued in bearer form;
- Counterparties who are involved in suspicious activities.

Counterparty Categorization Criteria

This Section defines the criteria for the categorization of Counterparties based on their risk. The Anti-Money Laundering Compliance Department shall be responsible for categorizing Counterparties in one of the following three (3) categories based on the criteria of each category set below:

Low Risk Counterparties

The Company may apply simplified due diligence to the following types of Counterparties provided that there is a low risk or no suspicion for money laundering and terrorist financing:

- credit or financial institution covered by the Regulations;
- credit or financial institution carrying out one or more of the financial business activities as these are defined by the Law and which is situated in a country outside the EEA, which:
 - ✓ in accordance with a decision of the VFSC, imposes requirements equivalent to those laid down by the Regulations, and
 - ✓ it is under supervision for compliance with those requirements
 - ✓ listed companies whose securities are admitted to trading on a Regulated Market in a country of the EEA or in a third country which is subject to disclosure requirements consistent with community legislation
 - ✓ domestic public authorities of countries of the EEA.

It is provided that further to the cases mentioned above, the Company has to gather sufficient information to establish if the Counterparty qualifies as a low-risk one. In this respect, the

Compliance Officer (CO) shall be responsible to gather the said information. The said information shall be duly documented and filed.

Normal Risk Counterparties

The following types of Counterparties can be classified as normal risk Counterparties with respect to the Money Laundering and Terrorist Financing risk which the Company faces:

- any Counterparty which does not fall under the ‘low risk Counterparties’ or ‘high risk Counterparties’ categories set above, respectively.

High Risk Counterparties

The following types of Counterparties can be classified as high risk Counterparties with respect to the Money Laundering and Terrorist Financing risk which the Company faces:

- Counterparties who are not physically present for identification purposes (non-face-to-face Counterparties);
- Trust accounts;
- PEPs’ related accounts;
- Counterparties from countries which inadequately apply FATF’s recommendations;
- any other Counterparties that their nature entail a higher risk of money laundering or terrorist financing;
- any other Counterparties determined by the Company itself to be classified as such.

Enterprise-wide risk assessment

As part of its risk-based approach, <https://betsolutions.com/> has conducted an AML “Enterprise-wide risk assessment” (EWRA) to identify and understand risks specific to <https://betsolutions.com/> and its business lines. The AML risk policy is determined after identifying and documenting the risks inherent to its business lines, such as the services the website offers. The Counterparties to whom services are offered, transactions performed by these Counterparties, delivery channels used by the bank, the geographic locations of the bank’s operations, customers and commerce, and other qualitative and emerging risks. The EWRA must be documented, approved by the board of directors, and reassessed yearly.

The identification of AML risk categories is based on <https://betsolutions.com/> understanding of regulatory requirements, regulatory expectations, and industry guidance. Additional safety measures are taken to take care of the other risks the world wide web brings with it.

The EWRA is yearly reassessed.

Due Diligence and Identification procedures

Cases for the application of Counterparty Identification and Due Diligence Procedures

The Company shall duly apply Counterparty identification procedures and Counterparty due diligence measures in the following cases:

- when establishing a Business Relationship
- when there is a suspicion of money laundering, proliferation financing or terrorist financing, regardless of the amount of the transaction
- when there are doubts about the veracity or adequacy of previously Counterparty identification data.

In this respect, it is the duty of the CO, to apply all the relevant Counterparty Due Diligence Identification Procedures for the three (3) cases mentioned above. Furthermore, the Administration/Back-Office Department shall also be responsible to collect and file the relevant Counterparty identification documents, according to the recording keeping procedures.

Further, the Back Office Department shall be responsible to maintain at all times and use during the application of Counterparty due diligence and identification procedures template-checklists with respect to required documents and data from potential Counterparties, as per the requirements of the Law and the Regulation.

Counterparty's identification documents and relevant information shall be updated on an annual basis or earlier if deemed necessary (e.g. in case of investigation of suspicious transactions etc.)

Ways of application of Counterparty Identification and Due Diligence Procedures

Counterparty identification procedures and Counterparty due diligence measures shall comprise:

- identifying the Counterparty and verifying the Counterparty's identity on the basis of documents, data or information obtained from a reliable and independent source;
- identifying the beneficial owner and taking risk-based and adequate measures to verify the identity on the basis of documents, data or information obtained from a reliable and independent source so that the person carrying on in financial or other business knows who the beneficial owner is; as regards legal persons, trusts and similar legal arrangements, taking risk based and adequate measures to understand the ownership and control structure of the Counterparty;
- obtaining information on the purpose and intended nature of the business relationship;
- conducting on-going monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the information and data in the

possession of the person engaged in financial or other business in relation to the Counterparty, the business and risk profile, including where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date.

Time of Application of the Counterparty Identification and Due Diligence Procedures

With respect to the timing of the application of the Counterparty Identification and Due Diligence Procedures, the CO shall be responsible for the application of the following provisions:

- The verification of the identity of the Counterparty and the Beneficial Owner shall be performed before the establishment of a Business Relationship or the carrying out of a transaction.
- By way of derogation from point (1) above, the verification of the identity of the Counterparty and the Beneficial Owner shall be completed during the establishment of a Business Relationship if this is necessary not to interrupt the normal conduct of business and where the risk of money laundering or terrorist financing occurring is low. In such situations these procedures shall be completed as soon as possible after the initial contact and before any transactions are conducted.
- In cases where the Company is unable to comply with points 1 and 2, the Company shall not carry out any transaction, establish a Business Relationship or carry out an Occasional Transaction and consider making a report to the FIU.
- Identification procedures and Counterparty due diligence requirements shall be applied not only to all new Counterparties but also to existing ones at appropriate times, depending on the level of risk of being involved in money laundering or terrorist financing.

Ongoing transaction monitoring

AML-Compliance ensures that an “ongoing transaction monitoring” is conducted to detect transactions that are unusual or suspicious.

This transaction monitoring is conducted on two levels:

1) The first Line of Control:

<https://betsolutions.com/> works solely with trusted Payment Service Providers who all have effective AML policies in place to prevent the large majority of suspicious deposits onto <https://betsolutions.com/> from taking place without proper execution of KYC procedures onto the potential Counterparty.

2) The second Line of Control:

<https://betsolutions.com/> makes its network aware so that any contact with the Counterparty must give rise to the exercise of due diligence on transactions on the account concerned. In particular, these include:

- Requests for the execution of financial transactions on the account;
- Requests concerning means of payment or services on the account.

Also, the verification with adjusted risk management should provide all necessary information about all Counterparties of <https://betsolutions.com/> at all times.

Also, all transactions must be overseen by employees overwatched by the AML compliance officer, who the general manager overwatches.

The specific transactions submitted to the customer support manager, possibly through their Compliance Manager, must also be subject to due diligence.

Determination of the unusual nature of one or more transactions essentially depends on a subjective assessment concerning the knowledge of the customer (KYC), their financial behavior, and the transaction counterparty.

These checks will be done by an automated system, while an Employee crosschecks them for additional security.

The transactions for which it is difficult to gain a proper understanding of the lawful activities and origin of funds must, therefore, rapidly be considered atypical (as they are not directly justifiable).

Any <https://betsolutions.com/> staff member must inform the AML division of any atypical transactions which they observe and cannot attribute to a lawful activity or source of income known to the Counterparty.

3) The third Line of Control:

As the last line of defense against AML <https://betsolutions.com/> will do manual checks on all suspicious and higher-risk Counterparties to entirely prevent money laundering.

If fraud or Money Laundering is found, the authorities will be informed.

Reporting of Suspicious transactions on <https://betsolutions.com/>

In its internal procedures, <https://betsolutions.com/> describes in precise terms the attention of its staff members, when it is necessary to report and how to proceed with such reporting.

Reports of atypical transactions are analyzed within the AML team following the precise methodology fully described in the internal procedures.

Depending on the result of this examination and based on the information gathered, the AML team:

- will decide whether it is necessary or not to send a report to the relevant authorities;
- will decide whether or not it is necessary to terminate the business relations with the Counterparty.

The company and its employees are prohibited from disclosing the fact that an unusual transaction report (UTR) is being filed or that an investigation is underway (“tipping off”).

Procedures

The AML rules, including minimum KYC standards, will be translated into operational guidance or procedures that are available on the Intranet site of <https://betsolutions.com/>.

Record keeping

Records of data obtained for identification must be kept for at least ten years after the business relationship has ended.

Records of all transaction data must be kept for at least ten years following the carrying-out of the transactions or the end of the business relationship.

These data will be safe and encrypted, stored offline and online.

Training

<https://betsolutions.com/> human employees will make manual controls on a risk-based approval for which they get special training.

The training and awareness program is reflected by its usage:

- A mandatory AML training program at least annually following the latest regulatory evolutions for all in touch with finances
- Academic AML learning sessions for all new employees

The content of this training program has to be established by the kind of business the trainees are working for and the posts they hold. These sessions are given by an AML specialist working in the **BYTERIVERS N.V.** AML team.

Auditing

Internal audit regularly establishes missions and reports about AML activities.

The AML compliance program must be evaluated at least annually by a qualified independent party. The auditor must have at least two years of AML compliance experience and a relevant certification.

Data Security

All data given by any Counterparty will be kept secure and will not be sold or provided to anyone else. Only if forced by law or to prevent money laundering data may be shared with the AML authority of the affected state.

<https://betsolutions.com/> will follow all guidelines and rules of the data protection directive (officially Directive 95/46/EC)

Contact us

If you have any questions about our AML and KYC Policy, please get in touch with us through the section “Contact Us” on Website <https://betsolutions.com/>.

If you have any complaints about our AML and KYC Policy, please get in touch with us through the section “Contact Us” on Website <https://betsolutions.com/>.