

VAVADA

AML Compliance Policy

POL-AML-007-02

AML Compliance Policy

1. Introduction.....	2
2. Glossary of Terms.....	2
3. General Provisions.....	3
4. Responsibilities of the Client.....	4
5. Obligations of the Company.....	4
6. Know Your Client and Due Diligence.....	4
7. The List of Prohibited Parties to the Company Transactions.....	6
8. Responsibilities of MLRO.....	7
9. Risk Assessment.....	8
10. Training Process.....	8
11. Deposits and Withdrawals of the Client's funds.....	9
12. Miscellaneous conditions.....	9
13. Suspicious Activity Reporting.....	9
14. Identification of the Client.....	10
15. Client Risk-Based Approach.....	10
17. Ongoing monitoring.....	11
18. Transaction Monitoring.....	12
Appendix A: VAVADA B.V. Prohibited Jurisdictions.....	13

1. Introduction

The company VAVADA B.V., was registered on March 21, 2017, under registration number 143168 (O) with the registration address at Hanchi Snoa 19, Trias Building, Curacao. (hereinafter referred to as the "Company") establishes the Company's policy on countering the legalization (laundering) of money (hereinafter referred to as "AML") obtained by illegal means and financing terrorism (hereinafter referred to as "FT") (hereinafter referred to as "Company policy"). The present Company policy includes an information cluster on the identification and conscientiousness of the Client ("Due Diligence Policy" (hereinafter - DD) and "Know Your Client Policy" (hereinafter - KYC)).

2. Glossary of Terms

- 2.1. **AML (Anti-Money Laundering):** Measures and policies aimed at preventing the laundering of money obtained illegally and financing terrorism.
- 2.2. **FT (Financing Terrorism):** Financial support for acts of terrorism or terrorist organizations.
- 2.3. **Client:** An individual (natural person) using the Company's services
- 2.4. **Beneficial Owner:** By using the website, the Client confirms that they are the beneficial owner of the funds used for gaming purposes. A beneficial owner is defined as the individual (natural person) who ultimately owns or controls the funds or assets used in transactions or activities on the platform, acting solely on their own behalf without the involvement of any third party or intermediary.

- 2.5. **KYC (Know Your Client):** A policy for verifying and identifying Clients to assess their risk levels.
- 2.6. **DD (Due Diligence):** A process of investigation or auditing to ensure compliance with laws, regulations, and ethical standards.
- 2.7. **MLRO (Money Laundering Reporting Officer):** A designated individual responsible for overseeing and ensuring the implementation of AML policies and reporting suspicious activities.
- 2.8. **FATF (Financial Action Task Force):** An international organization that sets standards and promotes effective implementation of AML and FT measures.
- 2.9. **OFAC (Office of Foreign Assets Control):** A U.S. government agency that administers sanctions against designated individuals, groups, and entities.
- 2.10. **PEP (Politically Exposed Person):** An individual who holds or has held a high-ranking public office, along with their close associates and family members.
- 2.11. **STR/SAR (Suspicious Transaction Report/Suspicious Activity Report):** Reports filed to regulatory authorities when suspicious or unusual activities are detected.
- 2.12. **FIU (Financial Intelligence Unit):** A government agency responsible for collecting and analyzing information to combat financial crimes like money laundering and terrorism financing.
- 2.13. **Risk-Based Approach:** A method of assessing and managing risks based on their likelihood and impact, especially in Client relationships.
- 2.14. **Sanctioned List:** A list of individuals, entities, or countries subject to trade restrictions or financial penalties.
- 2.15. **Prohibited Jurisdictions:** Countries or regions where the Company is not permitted to conduct transactions due to legal or regulatory restrictions.

3. General Provisions

- 3.1. The present Company policy is aimed at preventing the legalization (laundering) of proceeds obtained by criminal means, giving legal form to owning, using, or disposing of cash assets or other property obtained as a result of committing the crime by means of using the Company's services.
- 3.2. The company strictly adheres to AML/FT measures outlined in Curacao's AML legislation, including:
 - 3.2.1. Identification of beneficial owners as per GCB's AML/CTF guidance.
 - 3.2.2. Real-time transaction monitoring systems to prevent layering, placement, and integration of illicit funds.
 - 3.2.3. Filing STRs and SARs in accordance with FIU Curacao guidelines.
- 3.3. The Clients are exclusively individuals, excluding any legal entities or their representatives from access to the Company's services
- 3.4. The Clients are exclusively individuals acting on their own behalf. Company does not accept any activities and/or transactions on behalf of a third party.

4. Responsibilities of the Client

- 4.1. The Client undertakes to comply with the legislation of Curacao, the state of residence of the Client, as well as international provisions aimed at combating illegal trade, AML, and FT.
- 4.2. The Client undertakes to exclude direct or indirect participation in activities specified in paragraph 2.1 and any other illegal actions, including using information and telecommunication technologies, audiovisual and other programs, and technical means for unlawful purposes.
- 4.3. The Client undertakes to guarantee and confirm the legitimacy of the sources of origin of the Client's funds involved in the Company's Services, and other property of the Client, and affirm title to the Client's funds and property, or right of possession and right of use.
- 4.4. The Client undertakes to provide valid government-issued identification documents (e.g., passports, residency permits) for verification.
- 4.5. The Client undertakes to submit the documents specified in paragraph 2.4 with a duly certified translation into English if documents for identification of the Client are compiled and presented in full or in any part in another language.
- 4.6. The Client undertakes to perform other duties to the Company in accordance with the applicable legislation, international treaties, other international standards, the present Company Policy, and other internal local acts of the Company.

5. Obligations of the Company

- 5.1. The Company undertakes to observe the laws of the state of registration, and international provisions aimed at combating illegal trade, AML, and FT.
- 5.2. The Company undertakes to comply with the prohibition on informing the Clients and other persons about applicable measures of AML and FT, as well as providing advice on the necessity to submit documents on the grounds provided for by legislation, and on committing other actions that will not allow the Company to put in place AML/FT measures.
- 5.3. The Company undertakes to cooperate with the competent authorities of the states-residents at the stages of collection of information, preliminary investigation, court proceedings, and execution of court decisions on the available facts to assume (assert) the violation of AML and FT requirements by the Clients.
- 5.4. The Company undertakes to maintain the confidentiality of information about internal acts of the Company developed and applied for the purposes of AML and FT unless otherwise provided by law.
- 5.5. The Company undertakes to fulfill other requirements stipulated by the legislation of the resident states, international standards aimed at combating illegal trade, AML, and FT.
- 5.6. The Company ensures that any agents, affiliates, or third parties processing payments on behalf of the Company comply with AML requirements, including Customer Due Diligence (CDD) and record-keeping obligations.

6. Know Your Client and Due Diligence

- 6.1. The Company implements a unified KYC (Know Your Client) and Due Diligence process aimed at verifying the identity of Clients, assessing risks, and ensuring compliance with AML/FT legislation. These procedures apply exclusively to individuals who are the Company's Clients.

6.2. Clients are required to:

- 6.2.1. Provide valid government-issued identification documents (e.g., passport, ID card, or residence permit).
- 6.2.2. Confirm the legitimacy of the source of funds by submitting supporting evidence (e.g., bank statements, proof of salary, declarations regarding employment, business activity, or other sources of wealth).
- 6.2.3. Comply with all requests for additional information or documentation to verify their identity or source of funds.

Failure to comply with these requirements may result in the termination of services or reporting to the relevant authorities.

6.3. The Company conducts Client identification procedures directly or through authorized partner companies specializing in KYC services. These procedures include:

6.3.1. Collection of Identification Information:

- Full name, date of birth, nationality, and residence address.
- Valid government-issued identification documents (e.g., passport, ID card, residence permit).
- Proof of address (e.g., utility bill, bank statement).

6.3.2. Verification of Information:

- Cross-checking provided data with external legal databases, public records, and international sanctions lists (e.g., OFAC, EU, UN).
- Utilizing partner companies to perform KYC verification, including biometric checks, facial recognition, and validation of documents, where applicable.

6.3.3. Accuracy and Validity of Documents:

- Ensuring all identification documents are up-to-date and valid.
- Requiring translation of documents into English when necessary.
- Legalization or apostille of documents issued by foreign authorities, as per applicable laws.

6.3.4. Responsibilities of Partner Companies:

- Partner companies are required to adhere to the same AML/FT standards as outlined in the Company's policy and applicable local and international legislation.
- The Company maintains oversight of all KYC processes performed by partners, including periodic audits and reviews of their procedures.

6.3.5. Client Notification:

- Clients are informed that their data may be processed by authorized third-party KYC providers to verify their identity and ensure compliance with AML/FT requirements.

- 6.4. For high-risk Clients, including Politically Exposed Persons (PEPs), additional measures are applied:
- 6.4.1. Identification and verification of the source of wealth (SoW) and source of funds (SoF).
 - 6.4.2. Approval from senior management before establishing or continuing the business relationship.
 - 6.4.3. More frequent and detailed transaction monitoring.
 - 6.4.4. Screening against international sanctions lists (UN, EU, OFAC, and local Curaçao lists) on a quarterly basis.
- 6.5. The Company continuously monitors Client activity and transactions to:
- 6.5.1. Identify unusual patterns of behavior inconsistent with the Client's profile.
 - 6.5.2. Detect potentially suspicious transactions, such as:
 - 6.5.3. Large, frequent, or unusual deposits or withdrawals.
 - 6.5.4. Transactions involving high-risk jurisdictions.
 - 6.5.5. Report suspicious activities to the relevant authorities within the required timeframes.
- 6.6. The Company reserves the right to refuse service or terminate existing relationships if:
- 6.6.1. The Client refuses to provide the required identification documents or submits false information.
 - 6.6.2. The Client's activities or transactions raise reasonable suspicions of money laundering, terrorism financing, or other illegal activities.
- 6.7. All Client identification and transaction records are securely stored for at least five years, in compliance with applicable local laws and international AML standards.

7. The List of Prohibited Parties to the Company Transactions

- 7.1. The company operates in various jurisdictions and is subject to the laws of other countries. Of note is the U.S. Office of Foreign Assets Control ("OFAC") which administers the various laws that prohibit the conduct of business with hostile nations and blocked persons. Severe civil and criminal penalties exist for violations of these laws. OFAC provides financial institutions with a comprehensive master list of blocked persons and entities ("Blocked Persons"). Vavada B.V. is prohibited from engaging in transactions involving entities from this list, or other entities subject to international sanctions under OFAC.
- OFAC makes public the embargoed nations and alphabetical master lists of Blocked Persons ("OFAC lists"). The OFAC lists are amended from time to time and are available on OFAC's website at <http://www.treas.gov/offices/enforcement/ofac>.
 - UK sanctions list in website at <https://www.gov.uk/government/publications/the-uk-sanctions-list>
 - Consolidated list of persons, groups, and entities subject to EU financial sanctions

<https://data.europa.eu/euodp/en/data/dataset/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions>

- Curacao sanctions list in website at
<http://mot.cw/web/motweb/motweb.nsf/web/home?opendocument>

- 7.2. Each time a Client attempts to conduct a transaction, Vavada B.V.'s processes compare the name of the prospect against each of these lists, in addition to similar lists maintained by the United Nations, Australia, Canada, the European Union, the UK, Curacao, and other countries.
- 7.3. The Company assigns responsibility to the Money Laundering Reporting Officer (MLRO) to review and resolve potential matches flagged during the screening process. Clear "false positives" are dismissed after proper verification.
- 7.4. Transactions involving a true match must be reported to the regulatory entity responsible for placing that party on the respective list. In some cases, the law may require any funds to be submitted to the government entity responsible for the respective sanctions, while in others Company may simply hold funds until further instructions are provided by the regulatory entity. Usually, prior to releasing a transaction, Vavada B.V. will need to obtain additional Client information to assist in the evaluation process.
- 7.5. In addition, the Company complies with the requirements of responsive games and checks the lists of persons who have introduced themselves as people with addiction to prevent them from creating an account.

8. Responsibilities of MLRO

- 8.1. The nominated MLRO is responsible for the following key areas to ensure effective AML compliance:
 - 8.1.1. Suspicious Activity Reporting: Assessing whether there is sufficient suspicion to file reports of money laundering or terrorism financing and promptly disclosing these reports to the relevant authorities (e.g., FIU Curacao).
 - 8.1.2. Risk Management: Conducting risk assessments, identifying weaknesses in compliance processes, and implementing corrective measures to mitigate identified risks.
 - 8.1.3. Legislative Updates: Monitoring updates to AML/FT regulations and adapting Company policies and procedures accordingly.
 - 8.1.4. Client Support: Overseeing the application of Due Diligence policies, providing clear guidance to Clients regarding KYC requirements, and ensuring compliance.
 - 8.1.5. Employee Training: Developing and delivering comprehensive AML training programs, including periodic refreshers, to all employees.
 - 8.1.6. Regulatory Compliance: Ensuring full adherence to applicable AML/FT laws and regulations, including FATF Recommendations and national legislation.
 - 8.1.7. KYC Enforcement: Supervising the accurate and timely completion of all KYC procedures for Clients.
 - 8.1.8. Reporting: Submitting periodic compliance reports to external authorities (e.g., FIU, FATF) and internal Company management.

- 8.2. The MLRO ensures compliance with all applicable AML/FT legislation and is accountable for mitigating risks, avoiding penalties, and ensuring the Company's adherence to international standards.
- 8.3. When evidence or reasonable grounds for money laundering or terrorism financing are identified, the MLRO must:
 - 8.3.1. Promptly disclose the information to the relevant authorities as required by law.
 - 8.3.2. Maintain records of all disclosures and ensure they meet regulatory requirements.
- 8.4. The MLRO is authorized to request additional information or documentation from employees, stakeholders, or Clients to clarify potential compliance issues.
- 8.5. The MLRO monitors the implementation of AML/FT measures, ensuring timely investigations and the application of sanctions or corrective actions in case of violations.

9. Risk Assessment

- 9.1. The Company should access all available and potential risks of money laundering and terrorism financing, which also includes risks related to Clients, counterparties, and partners. Risk assessment should be provided considering geographic areas, countries of registration, services, and products.

In order to make a full assessment of the Client, the Company is authorized to collect the data and information, identifying the Client; record and keep the Client information by means, prescribed by applicable legislation; apply risk-based measures to verify the identity of the Client; to check the Client's identification information with lists of suspected terrorists, against United Nations and other relevant sanctions lists.

- 9.2. The Company is authorized to issue risk assessment questionnaires or forms for its Clients for the collection and subsequent analysis of information.
- 9.3. Strict adherence to AML Compliance is achieved by the effective system of tools and methods of control, aimed at continuous monitoring and updating of data and information, and, a system of managing and reducing identified risks and the timeliness and effectiveness of the measures taken to eliminate them.
- 9.4. The Company keeps a set of risk-mitigating measures, regulations, policies, training, and procedures.

10. Training Process

- 10.1. The Company maintains, develops, and implements on an ongoing basis a training process aimed at maintaining, developing, and updating AML awareness.
- 10.2. The training process includes briefings, in-class training, online training, webinars, digests, and instructions.
- 10.3. New employees of the Company shall receive anti-money laundering training as part of the mandatory new joiners introductory training program, MLRO is responsible for the provision of clarifications and detailed information on the requests of such new employees.
- 10.4. Each employee of the Company should be aware of their importance in ensuring that all measures designed to minimize risks and protect the Company from such risks are implemented.

- 10.5. All employees are required to conduct the annual Company's AML training and apply the acquired knowledge and recommendations in daily work.
- 10.6. Upon the request of the head/manager of the department, MLRO should organize individual training or briefing for the separate nominated employees.
- 10.7. The Company is authorized to conduct testing among employees to determine the level of their knowledge and understanding of mechanisms and tools of AML responsibilities.

11. Deposits and Withdrawals of the Client's funds

- 11.1. Similarly, in case of withdrawal of funds, the name of the Recipient Client should coincide with the name of the Sender Client, who simultaneously acts as the owner of the account from which the funds are debited.
- 11.2. In case of a bank transfer, the account from which the transaction was executed should coincide with the account to which the funds are transferred. In the case of online transfers, the accounts of deposit and withdrawal should also be the same.

12. Miscellaneous conditions

- 12.1. The Clients of the Company are informed and understand that the legal norms of the resident state that are parties to international acts and international treaties on AML and FT may be applied to legal relations between them.
- 12.2. If the employees of the Company use the Company's Services, they are subject to the provisions of the legislation, the present Company Policy on AML and FT, and other internal acts of the Company.
- 12.3. The Client undertakes to comply with the present Company Policy in full and, in the event of non-compliance in full, or in part, bears legal responsibility established by the applicable legislation, including for unfair and unconscientious actions of all other persons provided for by the Company Policy.

13. Suspicious Activity Reporting

- 13.1. The main goal of STR/SAR filings is to help the government identify individuals, groups, and organizations involved in fraud like terrorist financing, money laundering, and other crimes.
- 13.2. The Company implements and applies FATF Recommendations in its activities and relations with Clients.
- 13.3. The MLRO is obliged to conduct proper registration of the Company in go AML at FIU Curacao through which the suspicious transaction report (STR) or a suspicious activity report (SAR) is made.
- 13.4. A suspicious transaction report (STR) or a suspicious activity report (SAR) is filed by MLRO of the Company to FIU Curacao if MLRO has reasonable grounds to believe that a transaction is related to criminal activity.
- 13.5. While identifying unusual transactions, MLRO should use the Indicators List published by FIU Curacao.
- 13.6. All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.

- 13.7. MLRO is obliged to inform FIU Curacao regarding any suspicious transactions or activities without delay but in any case, no later than 48 hours after the transaction has been executed, or after there has been an intention for a transaction - for reports based on an objective indicator and 24 hours - for reports based on a subjective indicator.
- 13.8. If FIU Curacao, after proper analysis of an unusual transaction, concludes that there is a suspicion of money laundering and/or terrorism financing, this transaction will be reported to the Public Prosecutor's Office as a suspicious transaction. The FIU functions as an administrative buffer between the reporting entities on the one hand and the Public Prosecutor's Office on the other hand. This buffer prevents transaction information submitted by the reporting institutions from being unconditionally forwarded to the investigation services: only if there is a reasonable presumption of money laundering and/or financing of terrorism, will the data be furnished to the office of the Public Prosecutor.

14. Identification of the Client

- 14.1. The company collects certain Client's identification information from each Client who opens an account for example a copy of a government-issued identity document such as an ID card, passport, residence permit, driver's license, etc.
- 14.2. The company utilizes risk-based measures to verify the identity of each Client who opens an account; records the Client's identification information and the verification methods and results; provides the required Client identification notice to Clients that we will seek identification information to verify their identities; and compares Client's identification information with the list of prescribed persons that are believed to be involved in terrorism.
- 14.3. The company uses open-source due diligence methods like finding and analyzing publicly available information by using a combination of electronic and on-site public records (if available). This will help to ensure that the Company has the most complete and accurate information possible and, therefore, conducts a reliable and comprehensive risk assessment.

15. Client Risk-Based Approach

- 15.1. In order to detect suspicious activity, monitoring, and reporting, the Company uses the risk-based approach. The company assesses the core risk factors at minimum, such as the categories of Clients onboarded (particularly high-risk Clients), transactions, the jurisdictions they operate in, and the interface and delivery channels used.
- 15.2. The company examines each risk on the inherent and residual lever as per the Risk Assessment herein attached and as Appendix B which forms an integral part of this Policy.
- 15.3. It procures checks on Politically Exposed Persons (PEP), their family members, and close associates. We consider all types of PEPs - Foreign, Domestic, and International. PEP status applies for a period of 12 months after PEP the leaves their political role.
- 15.4. In line with the risk-based approach, extra Client Due Diligence measures undertaken by us to suspect any heightened Client risk factors, for example: Client, geography, product/service/interface risks. Client Due Diligence is conducted by asking Clients to provide identity documentation or general information that may be necessary to achieve certain objectives during the course of the Client relationship, such as:
- 15.4.1. To additionally verify and validate the Client's identity.
- 15.4.2. To update more regularly the information held on the Client.

- 15.4.3. To obtain additional information evidencing the Client's location, occupation, and source of wealth/funds.
- 15.5. In cases when money laundering is detected, the suspicious transaction report needs to be filed with the relevant authority.

16. Data Collection

- 16.1. The Company ensures secure collection, processing, and storage of data to comply with AML/FT legislation, verify Client legitimacy, and facilitate investigations by relevant authorities. The following types of data are maintained:
 - 16.1.1. **Client Data:** Identification and verification information, including passport/ID details, citizenship, name, date and place of birth, address, and proof of funds where applicable.
 - 16.1.2. **Employee Records:** Documentation of AML training completion, including dates and details of training sessions.
 - 16.1.3. **Internal and External Reports:** Suspicious Transaction Reports (STRs), Suspicious Activity Reports (SARs), and other compliance-related documentation.
 - 16.1.4. **Regulatory Correspondence:** Records of communication with authorities, such as FIU Curacao and other relevant bodies.
 - 16.1.5. **Compliance Monitoring Logs:** Documentation of the Company's internal controls and audits related to AML measures.
- 16.2. The Company retains all records for a minimum of five (5) years following the termination of the Client relationship or transaction, or longer if required by applicable legislation.
- 16.3. All records are processed in compliance with data protection laws and secured using appropriate technical and organizational measures to prevent unauthorized access, data loss, or breaches. These measures include:
 - 16.3.1. Encryption of sensitive data during storage and transmission.
 - 16.3.2. Regular audits of data storage systems.
 - 16.3.3. Access control measures to limit data access to authorized personnel only.
- 16.4. The Company ensures that data retention policies are reviewed periodically, and data is securely deleted or anonymized when no longer required.

17. Ongoing monitoring

- 17.1. The Company implements an ongoing monitoring process to ensure compliance with AML/FT requirements and to detect suspicious activities. Monitoring is conducted as follows:
 - 17.1.1. **Data and Document Updates:** Regularly reviewing and updating Client records to ensure they remain accurate, relevant, and consistent. Any discrepancies or outdated information are promptly investigated and resolved.
 - 17.1.2. **Transaction Monitoring:** Analyzing Client transactions to ensure they align with the Client's known profile, declared activities, and initial risk assessment.
- 17.2. Monitoring activities focus on identifying the following red flags:

- 17.2.1. Transactions or behaviors inconsistent with the Client's usual pattern or declared profile.
- 17.2.2. Unusual transaction volumes, frequencies, or amounts that exceed the expected activity.
- 17.2.3. Suspicious activities require the filing of a Suspicious Transaction Report (STR) with the relevant authorities (e.g., FIU Curacao).

18. Transaction Monitoring

The Company implements robust transaction monitoring procedures to detect, review, and report transactions that may indicate money laundering, terrorism financing, or other illicit activities. Monitoring is conducted using a combination of automated systems and manual oversight.

- 18.1. Customer Due Diligence (CDD) Threshold
 - 18.1.1. Any single transaction or a series of linked transactions exceeding NAf 4,000 (or equivalent) require Customer Due Diligence (CDD).
 - 18.1.2. Transactions that appear structured (multiple small deposits within a short period) to avoid CDD thresholds will be flagged for further review.
- 18.2. Enhanced Due Diligence (EDD)
 - 18.2.1. Enhanced Due Diligence (EDD) is required for any transaction equal to or exceeding NAf. 5,000 (or equivalent).
 - 18.2.2. EDD must also be conducted if the client is classified as high-risk, including but not limited to:
 - Politically Exposed Persons (PEPs).
 - Clients from high-risk jurisdictions.
 - 18.2.3. EDD measures include additional verification of Source of Funds (SoF).
- 18.3. Reporting to FIU Curacao

The Company is required to report any transaction deemed unusual or suspicious to FIU. The following transactions are classified as unusual:

- 18.3.1. Transactions that are presumed to be related to money laundering or terrorist financing, or have been reported to the Police or the Department of Justice in connection with such activities;
 - 18.3.2. Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
 - 18.3.3. Transactions in the amount of NAf. 5,000 or more.
- 18.4. Transaction Screening and Red Flags

The Company actively monitors transactions for red flags, including but not limited to:

- 18.4.1. Unusual transaction volumes or patterns inconsistent with a Client's risk profile.

-
- 18.4.2. Repeated attempts to deposit/withdraw just below reportable thresholds.
 - 18.4.3. Transactions linked to high-risk jurisdictions, sanctioned individuals, or politically exposed persons (PEPs).
 - 18.5. Record Keeping and Compliance
 - 18.5.1. All flagged transactions, investigations, and reports must be documented and securely stored for at least five (5) years.
 - 18.5.2. Transaction monitoring data must be accessible to FIU Curacao and regulatory authorities upon request.
 - 18.5.3. The Company ensures that all transaction data and reports are stored securely in compliance with data protection regulations to prevent unauthorized access or breaches.

Appendix A: VAVADA B.V. Prohibited Jurisdictions

COUNTRIES:		
Abkhazia	Guyana	Tristan da Cunha
Afghanistan	Haiti	Saint Kitts and Nevis
American Samoa	Hong Kong	Saint Vincent and the Grenadines
Anguilla	Iran	Saint-Martin
Antigua and Barbuda	Iraq	Saint-Pierre and Miquelon
Aruba	Isle of Man	Sao Tome and Principe
AUSTRALIA	Jersey	Serbia
Azad Kashmir	Kosovo	Seychelles
Barbados	Libya	Sierra Leone
Bermuda	Lugansk People's Republic	Singapore
Bonaire	Macau	Sint Eustatius
British Virgin Islands	Malawi	Sint Maarten
Canada	Marshall Islands	Slovakia
Cape Verde	Martinique	Solomon Islands
Cayman Islands	Mayotte	Somalia
Chad	Montenegro	South Ossetia
Christmas Island	Montserrat	South Sudan
Cocos (Keeling) Islands	Myanmar	State of Palestine
Comoro Islands	Netherlands	Sudan
Cook Islands	New Caledonia	Sweden
Cuba	Niue	Syria
Curacao	Norfolk	Turkish Republic of Northern Cyprus
Donetsk People's Republic	North Korea	Tokelau
East Timor	Northern Mariana Islands	Transnistria
Eritrea	Palau	Trinidad and Tobago
Falkland Islands	Pitcairn	Turks and Caicos Islands
Faroe Islands	Portugal	Tuvalu
Federated States of Micronesia	Republic of Artsakh	Uganda
France	Republic of the Congo	United Kingdom
French Guiana	Réunion	United States of America (USA)
Germany	Crimea	Vatican City
Gibraltar	Rwanda	Virgin Islands of the United States
Grenada	Saba	Wallis and Futuna
Guadeloupe	Sahrawi Arab Democratic Republic	Yemen
Guam	Saint Barthelemy	Belgium
Guernsey	Saint Helena, Ascension and	Spain
South Africa	Nigeria	Cambodia
China	Saudi Arabia	Switzerland
Lithuania		