



## ASPRO N.V

Dr. H. Fergusonweg 1, Curacao

### Anti-Money Laundering and Counter Terrorism Financing Policy

Approved by the Board of Directors

|                            |              |                                                                            |                                         |                                       |
|----------------------------|--------------|----------------------------------------------------------------------------|-----------------------------------------|---------------------------------------|
| <b>Company Name</b>        | Aspro N.V.   | Aspro N.V.                                                                 | Aspro N.V.                              | Aspro N.V.                            |
| <b>Version</b>             | 2024/V.1     | 2024/V.2                                                                   | 2025/V.3                                | 2025/V.4                              |
| <b>Date of Approval</b>    | January 2024 | November 2024                                                              | May 2025                                | December 2025                         |
| <b>Changes implemented</b> | New version  | Amendments as per new AML/CFT/CPF regulations (effective as of 15.05.2024) | New AML/CFT/CPF applicable January 2025 | Updates and Enhancement of the policy |

|                                            |                                                                                                                                                                     |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Authorized signatory</b><br>09.12. 2025 | <br><b>(SMES)</b><br><b>Solutions for Management and Employment Support N.V.</b> |
| <b>Compliance officer</b>                  | Rebecca Taiwo Owolabi<br><a href="mailto:compliance@aspronv.com">compliance@aspronv.com</a>                                                                         |

*This Policy is subject to copyright law and any reproduction of all or part of the contents in any form is prohibited.*

## Contents

|                                                                |    |
|----------------------------------------------------------------|----|
| Policy Statement .....                                         | 4  |
| Key Definitions.....                                           | 4  |
| Abbreviations .....                                            | 12 |
| Online Casino/Betting Environment .....                        | 12 |
| Senior Management Responsibilities .....                       | 13 |
| Money Laundering .....                                         | 13 |
| Key Stages of Money Laundering .....                           | 14 |
| Terrorist Financing .....                                      | 15 |
| Proliferation Financing.....                                   | 17 |
| National Risk Assessment (NRA) Integration.....                | 20 |
| Risk Score Calculation .....                                   | 21 |
| Unacceptable Clients .....                                     | 23 |
| ML & TF, PF Risk Assessment .....                              | 23 |
| Customer Risk .....                                            | 25 |
| Risk Based Approach (ML/ TF risks' detection) .....            | 25 |
| Transactional Risk Exposure .....                              | 26 |
| Geographical Risk Considerations .....                         | 27 |
| Distribution Channel Risk and Authentication Controls .....    | 28 |
| Technological Developments Risk Assessment.....                | 28 |
| Implementation of Mitigation Strategies .....                  | 29 |
| Compliance Officer.....                                        | 32 |
| Customer Due Diligence Guidelines .....                        | 33 |
| Transaction Monitoring .....                                   | 43 |
| Customer Acceptance Policy (CAP) .....                         | 45 |
| Enhanced Due Diligence.....                                    | 47 |
| PEPs (Politically Exposed Persons) .....                       | 48 |
| Ongoing Monitoring .....                                       | 50 |
| Sanction Management, FATF Blacklist, License Restrictions..... | 55 |
| Record Keeping .....                                           | 56 |

Suspicious Activity Reporting ..... 57

Unusual Transactions ..... 59

Employee Training ..... 59

Audit Function ..... 64

Appendix I Score Calculation..... 67

Appendix II Employee Screening Program ..... 68

Appendix III Sanctions Policy ..... 73

## **Policy Statement**

The purpose of the Anti-Money Laundering Policy (the AML Policy) is to promote companywide compliance with the local and international Anti Money Laundering/ Counter Terrorism Funding (AML/CFT/CPF) legislation, implement best AML/CFT/CPF industry standards internally, and uphold all relevant laws in all the jurisdictions Aspro N.V. operates in. The AML Policy's framework is based on robust AML/CFT/CPF measures, including the identification and mitigation of the inherent risks associated with customers, products and services, payment methods, countries, and delivery channels.

The AML Policy has been approved by the Board of Directors (BoD) of Aspro N.V. and is subject to an annual review. In addition to the annual review process, periodic amendments of the policy are submitted to the BoD for approval when alterations in AML/CFT/CPF operator practices are advisable and/or a request to implement urgent internal and third party AML audit recommendations as regards risk probability and risk impact is put forward by a nominated officer.

The AML Policy is a reflection of the main international objectives highlighted by the current legislation in Curacao i.e. the upcoming National Ordinance for Games of Chance (LOK), the Criminal Code of Curacao, The National Ordinance on Offshore Games of Hazard ( PB 1993, no.63) ( NOOGH) as well as National Ordinance Penalization of Money Laundering (NOPML), the National Ordinance on the Reporting of Unusual Transactions (NORUT), and the National Ordinance on Identification of clients when Rendering Services (NOIS). It also relies on the international legislation and policy initiatives such as Recommendations of the Financial Action Task Force (The FATF Recommendations), the European Anti-Money Laundering Directives (the 4th, 5th and the 6th AMLDs), and the Wolfsberg Principles.

The Company's directors, officers and personnel are committed to upholding a set of standards set in the Policy in line with the recommendations of the AML/CFT/CPF supervisor in Curacao, namely the Curacao Gaming Control Board.

The Policy applies to all persons at all levels working for the Company and third party consultants whose services are enlisted from time to time for audit purposes.

## **Key Definitions**

**AML Policy** The Policy on Prevention of Money Laundering Terrorist Financing

**Anti-Money Laundering and Counter Financing of Terrorism Program** programs are established to fight against money laundering and terrorist financing and consist of written internal policies, procedures and controls, overseen by AML compliance team headed by Compliance officer, who is also responsible for AML training as well as arranging an independent review to audit the program.

**Alert** a notification that an analysis of red discrepancies is required based on defined red flags and underlying typologies.

**AML/CFT/CPF Supervisor** the Curaçao Gaming Control Board (GCB) and a relevant local master license holder where applicable.

**Automated Screening Tool (AST)** Software systems that automate the customers' screening process including against sanctions lists.

**Beneficial Owner** – a natural person who ultimately owns or controls an account through which a transaction is being conducted.

**Blacklist** An internal list of names (including places, persons, entities, and individuals) that are screened to identify any sanctions exposure, in addition to government and vendor-maintained sanctions lists.

**The FATF blacklist** is a list of countries that FATF has determined are noncooperative in the international fight against money laundering and terrorist financing.

**Comprehensive Sanctions** that prohibit all transactions and activity with a sanctioned country by the sanctioning country except in rare, specific instances.

**Criminal Proceeds** Any property derived from or obtained, directly or indirectly, through the commission of a crime. **Customer** a person that opens an account and transacts with the Company.

**Customer Relationship** a customer relationship, encompasses all contact with a prospective customer during onboarding and while using the Company's services and products.

**Customer Due Diligence** is a set of internal controls that internet gambling operator establish a customer's identity, predict with relative certainty the types of transactions in which the customer is likely to engage, and assess the extent to which the customer exposes it to a range of risks (i.e., money laundering and sanctions). Organizations also need to know their customers through CDD to guard against fraud and comply with the requirements of relevant legislation and regulation.

**"High-risk third country"** a third country, which is flagged by the European Commission under the provisions of paragraph (2) of Article 9 of the EU Directive by means of delegated powers and by FATF, and which has strategic deficiencies in its national AML/CFT/CPF regime that pose significant threats to the financial system of the Union, and a third country which is classified by the Company as high risk, according to the risk assessment referred to in Article 58a of the Law.

**Due Diligence** The investigation and examination of an individual customer or a legal entity, conducted in the process of preparing for a business transaction. Due diligence should be completed before initiating any transaction or business relationship.

**Economic Sanctions** The imposition of trade or financial restrictions and penalties by one or more countries against another country, entity, or individual with the purpose of changing a behavior. Economic sanctions can include actions such as tariffs, trade restrictions, and financial limitations.

**Egmont Group of Financial Intelligence Units** The Egmont Group consists of a numerous national of financial intelligence units (FIUs) that meet regularly to find ways to promote the development of FIUs and to cooperate, especially in the field of information exchange, training and the sharing of expertise. The goal of the group is to provide a forum for FIUs to improve cooperation in the fight against money laundering and the financing of terrorism, and to foster the implementation of domestic programs in this field.

**Embargo** An official government action to ban trade or commercial activity with a specific country, sometimes involving a specific trade product (e.g., a grain embargo or an oil embargo).

**Enhanced Due Diligence (EDD)** In conjunction with Customer Due Diligence, EDD calls for additional measures aimed at identifying and mitigating the risk posed by higher risk customers. It requires developing a more thorough knowledge of the nature of the customer, the customer's business and understanding of the transactions in the account than a standard or lower risk customer.

**European Union (EU)** The modern EU was founded in the Treaty of Maastricht on European Union, signed in 1992 and effective in 1993. The EU is a politico economic union of member states located primarily in Europe. European Union Directive on Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing First adopted by the European Union in June 1991 and updated in 1997, 2005, 2015, 2018 and 2020 the directive requires EU member states to prohibit and manage the risks of money laundering and terrorist financing.

**Exclusions List** A list of names that are excluded from the screening process. These are names that the compliance team has verified do not actually match a name on a sanctions list.

**Financial Action Task Force (FATF)** FATF was created in 1989 by the Group of Seven industrial nations to foster the establishment of national and global measures to combat money laundering. It is an international policymaking body that sets Anti-Money laundering standards and counterterrorist financing measures worldwide. Its Recommendations do not have the force of law. 35 countries and two international organizations are members. In 2012, FATF substantially revised its 40 + 9 Recommendations and reduced them to 40. FATF develops annual typology reports showcasing current money laundering and terrorist financing trends and methods.

**Financial Intelligence Unit (FIU)** A central national agency responsible for receiving, analyzing, and transmitting disclosures on suspicious transactions to appropriate authorities.

**First Line of Defense** within the governance structure of a sanction's compliance program, the first line of defense (also referred to as the "front line") includes relationship managers and other customer-facing employees who are closest to the customers and counterparties during the onboarding and contracting phase of relationships. The first line defense is responsible for ensuring that adequate information is obtained so that effective screening of customers and their owners and controllers can be performed. In general, the first line defense owns and manages the collection of SDD information.

**Grey list** A grey list is a list of entities that are suspicious or higher risk for causing a negative impact to a firm. Within the context of sanctions, the grey list includes the names of countries with strategic deficiencies in Anti-Money laundering and counterterrorism financing regimes. Moreover, these countries have also not made sufficient progress or otherwise committed to action plans to address deficiencies identified by FATF.

**Inherent Risk** The level of sanctions risks that exist before controls are applied to mitigate them. There are four main inherent risk categories: customers, products and services, countries, and delivery channels. Inherent risk is linked to the risk assessment process, which evaluates the effectiveness of an institution's risk controls. Inherent risk considers the likelihood and impact of noncompliance prior to considering any mitigating effects of risk management processes.

**Investigation** The process of obtaining, evaluating, recording, and storing information about an individual or legal entity with whom one is conducting business, in response to an alert indicating a possible sanctions violation. Investigations often begin with simple checks before progressing to further investigation such as account review, customer outreach, and possible escalation to the compliance function.

**Know Your Customer (KYC)** Anti-Money laundering policies and procedures used to determine the identity of a customer and the type of activity that is "normal and expected," and to detect activity that is "unusual" for a particular customer.

**Know Your Employee (KYE)** Anti-Money laundering policies and procedures for acquiring a better knowledge and understanding of the employees of an institution for the purpose of detecting conflicts of interests, money laundering, past criminal activity and suspicious activity.

**Layering** The second phase of the classic threestep money laundering process between placement and integration, layering involves distancing illegal proceeds from their source by creating complex levels of financial transactions designed to disguise the audit trail and to provide anonymity.

**Mandatory Sanctions Lists** Supranational sanctions lists, such as those including targets designated by the United Nations Security Council Resolutions (UNSCR), which must be screened against. Depending on the country in which a business is located and operates, local sanctions regimes may be required (i.e., mandatory) and would need to be included within a firm's sanctions compliance program.

**Minor** – under the 18 years of age.

**Money Laundering** The process of concealing or disguising the existence, source, movement, destination, or illegal application of illicitly derived property or funds to make them appear legitimate. It usually involves a three-part system: placement of funds into a financial system, layering of transactions to disguise the source, ownership and location of the funds, and integration of the funds into society in the form of holdings that appear legitimate. The definition of money laundering varies in each country where it is recognized as a crime.

**Money Laundering Reporting Officer (Compliance officer)** A term used in various international rules to refer to the person responsible for overseeing a firm's Anti-Money laundering activities and program and for filing reports of suspicious transactions with the national FIU. The Compliance officer is the key person in the implementation of Anti-Money laundering strategies and policies.

**Monitoring** An element of an institution's Anti-Money laundering program in which customer activity is reviewed for unusual or suspicious patterns, trends or outlying transactions that do not fit a normal pattern. Transactions are often monitored using software that weighs the activity against a threshold of what is deemed "normal and expected" for the customer.

**Office of Foreign Assets Control (OFAC)** the agency within the US Department of the Treasury responsible for administering and enforcing economic sanctions issued as part of US foreign policy and by international organizations like the United Nations against targeted foreign countries. It often works in consultation with other agencies, such as the Department of State, to oversee national security goals. A core component of the agency's responsibilities is the creation and maintenance of the Specially Designated Nationals (SDN) list.

**Politically Exposed Person (PEP)** According to FATF's revised 40 Recommendations of 2012, a PEP is an individual who has been entrusted with prominent public functions in a foreign country, such as a head of state, senior politician, senior government official, judicial or military official, senior executive of a state-owned corporation or important political party official, as well as their families and close associates. The term PEP does not extend to middle ranking individuals in the specified categories. Various country regulations will define the term PEP, which may include domestic as well as foreign persons.

**Proliferation Financing (PF):** Aspro N.V. is committed to identifying and mitigating the risk of proliferation financing (PF), defined as the provision of funds or financial services used for the manufacture, acquisition, or transfer of nuclear, chemical, or biological weapons and related materials. The Company incorporates PF risk indicators into its risk assessments and customer due diligence procedures in accordance with the FATF Recommendations and Curaçao's legal obligations. PF risks are assessed alongside AML/CFT/CPF risks and subject to ongoing monitoring, reporting, and escalation to the FIU where necessary.

**Red Flag (like alert)** A warning signal that should bring attention to a potentially suspicious situation, transaction or activity.

**Regulatory Agency** A government entity responsible for supervising and overseeing one or more categories of financial institutions. The agency generally has authority to issue regulations, to conduct examinations, to impose fines and penalties, to curtail activities and, sometimes, to terminate charters of institutions under its jurisdiction.

**Risk Appetite** The amount of risk that a firm is willing to accept in pursuit of value or opportunity. A firm's risk appetite reflects its risk management philosophy and comfort level for undertaking business in situations in which there could be an elevated sanctions risk. In turn, risk appetite influences the firm's culture and operating style and guides resource allocation. An organization's risk appetite is determined through the risk assessment process and formalized in a Risk Appetite Statement or Framework. A business should determine its risk appetite based on the resources it has to invest in controls, staffing, and measures to protect its reputation. Firms can have an overarching risk appetite (i.e., enterprise wide) and/or have risk appetites defined on a more granular level (e.g., by department).

**Risk Assessment** A tool that allows a business to identify and assess the extent to which it may be exposed to risks.

**Risk Based Approach** The assessment of the varying risks associated with different types of businesses, clients, accounts, and transactions to maximize the effectiveness of an Anti-Money laundering program.

**Second Line of Defense** The sanctions compliance function, the larger compliance function, and the human resources and technology departments comprise the second line of defense within the governance structure of a sanction's compliance program. The sanctions compliance officer ensures ongoing monitoring for sanctions compliance to enable the escalation of identified issues. In general, the second line exists to ensure that SDD procedures and processes applied by the first line are designed properly, firmly established, and applied as intended. The second line defense reviews the effectiveness of controls used to mitigate sanctions risks; provides information to the first line; and investigates possible noncompliance with sanctions restrictions.

**"Senior Management"** an officer or employee of the Company with sufficient knowledge of the Company's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure and need not to be a member of the Board of Directors.

**"Structuring"** small transfers or small deposit amounts from customers that are trying to avoid recordkeeping requirements or trigger AML flag alerts from any company (EMI).

**Sanctions** are punitive or restrictive actions taken by individual countries, regimes, or coalitions with the primary purpose of provoking a change in behavior or policy. Sanctions can restrict trade, financial transactions, diplomatic relations, and movement. They can be specific or general in their implementation and enforcement. Sanctions are also referred to as restrictive measures.

**Sanctions Evasion** The deliberate attempt to remove or conceal the involvement of sanctioned places, entities, or individuals in a transaction or series of transactions. When sanctions evasion is successful, a business that would have been flagged, taxed, restricted, or prohibited is allowed to proceed unhindered.

**Sanctions Due Diligence (SDD)** A similar process to Know Your Customer (KYC) / Customer Due Diligence (CDD) that focuses on the risks specific to sanctions, considering governance and risk assessment. SDD builds upon the KYC/CDD information an organization collects as part of its existing AML program. SDD is applied throughout the life cycle of a relationship at the start of a relationship (i.e., onboarding); when new products are introduced, in response to trigger events during a relationship, such as a "match" generated by a screening tool; during periodic reviews; and when a relationship ends.

**Sanctions List** A document or database listing individuals, legal entities, and countries with whom it is illegal to do business.

**Sanctions Regime** A set of sanctions that have a common nexus or theme. These are either referred to by the issuer of the set of sanctions or by the intended purpose of the set of sanctions. For example, the "OFAC sanctions regime" or the "North Korea sanctions regime." Depending on the context, a sanctions regime may be limited to unilateral sanctions or may include multilateral sanctions.

**Sanctions Compliance** The act of adhering to the sanctions related legislation, regulations, rules, and norms that make up the complex sanctions landscape.

**Simple Checks** One of the first steps in an investigation, simple checks are those initial actions taken to discount or confirm a sanctions link; an example of a simple check includes comparing data about a sanctions target with a firm's Know Your Customer (KYC) data.

**Specially Designated Nationals and Blocked Persons List (SDN List)** A list of individuals and companies, published by OFAC, that are owned, controlled by, or acting on behalf of a targeted country. The list also includes groups and people, such as terrorists or drug traffickers, who are associated with a specific crime as opposed to a country. The US Department of the Treasury maintains the list and may name a person or company as an SDN. When the government identifies a person or company as an SDN, it blocks their assets and forbids US persons to do business with them. The government may also impose fines and imprison lawbreakers.

**Suspicious Activity** irregular or questionable customer behavior or activity that may be related to a money laundering or other criminal offense, or to the financing of a terrorist activity. May also refer to a transaction that is inconsistent with a customer's known legitimate business, personal activities, or the normal level of activity for that kind of business or account.

**Suspicious Transaction Report (STR)** A government filing required by reporting entities that includes a financial institution's account of a questionable transaction. Many jurisdictions require financial institutions to report suspicious transactions to relevant government authorities such as its FIU on a suspicious transaction report (STR), also known as a suspicious activity report or SAR.

**Terrorist Financing** The process by which terrorists fund their operations in order to perform terrorist acts. There are two primary sources of financing for terrorist activities. The first involves financial support from countries, organizations or individuals. The other involves a wide variety of revenue generating activities, some illicit, including smuggling and credit card fraud.

**Third Line of Defense** The third line defense within the governance structure of a sanction's compliance program is the internal audit, which involves independent reviews of the controls applied by the first two lines of defense. It independently evaluates the risk management and controls of the bank through periodic assessments, including the adequacy of the bank's controls to mitigate the identified risks. It also evaluates the effectiveness of the staff's execution of the controls, the effectiveness of the compliance oversight and quality controls, and the effectiveness of the training.

**Third Party Database** Third party databases can be a good source of both primary and secondary information sources. Examples of third party databases include rating agencies, stock exchanges, and legal databases.

**Unilateral Sanctions** These are sanctions imposed by a single country against a targeted entity. These are generally considered less effective than multilateral sanctions. Still, they serve to target specific offensive practices on behalf of imposing nations.

**United Nations (UN)** An international organization that was established in 1945 by 51 countries committed to preserving peace through cooperation and collective security. Today, nearly every nation in the world belongs to the UN. See also Vienna Convention. The United Nations contributes to the fight against organized crime with initiatives such as the Global Program against Money Laundering (GPML), the key instrument of the UN Office of Drug Control and Crime Prevention in this task. Through the GPML, the UN helps member states to introduce legislation against money laundering and to develop mechanisms to combat this crime.

**Unusual Transaction** - Transaction that appears designed to circumvent reporting requirements, is inconsistent with the account's transaction patterns or deviates from the activity expected for that type of account.

**Wolfsberg Group** an association of global financial institutions, including Banco Santander, Bank of America, Bank of Tokyo Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse Group, Deutsche Bank, Goldman Sachs, HSBC, J.P. Morgan Chase, Société Générale, Standard Chartered Bank and UBS. In 2000, along with Transparency International and experts worldwide, the institutions developed global Anti-Money laundering guidelines for international private banks.

## Abbreviations

**AML** – Anti-Money Laundering

**Compliance Officer.** A senior officer at management level and independent from the game's operations, responsible for the detection and deterrence of money laundering and terrorist financing.

**BoD** – Board of Directors of the Company

**CDD Customer Due Diligence**

**EDD Enhanced Due Diligence**

**CFT** Combating the Financing of Terrorism

**EU** – European Union

**FATF** – Financial Action Task Force

**NOOGH** The National Ordinance on Offshore Games of Hazard (Landsverordening buitengaatsse hazardspelen, P.B. 1993, no. 63)

**PEP** Politically Exposed Person

**UN** United Nations

## Online Casino/Betting Environment

Aspro N.V., a legal entity established in Curaçao. Company is licensed under Curaçao Gaming Control Board with license number OGL/2024/565/0553 issued 11/11/2024. This license mandates compliance with Curaçao's regulatory requirements and imposes strict restrictions on service provision in specific jurisdictions. As such, Aspro N.V., refrains from offering remote gaming services in the United States, Australia, Dutch West Indies (Aruba, Bonaire), Curaçao, France, Germany, the United Kingdom, Belize, and the Netherlands. The company strictly adheres to this policy, operating exclusively in regions where online gambling is legally permitted, without targeting markets where such activities are prohibited.

E-Gaming and betting operators are susceptible to the money laundering risks spanning identity theft and fraud, structuring, layering and collusion of the employees with the customers or the external payment providers to help them bypass internal safeguards.

## **Senior Management Responsibilities**

The Company's senior management is fully engaged in the process of assessment of inherent risk categories. It is required by the Board of Directors that a nominated AML/CFT/CPF Officer regularly updates the Members on any significant deviations related to the control environment and produces an annual report covering the operator's systems and controls that mitigate the risks of money laundering, terrorist financing and proliferation financing. Periodic reviews of the relevant policies and procedures take place at least every 6 months based on monthly risk assessments' results and the AML/CFT/CPF Officer may request the approval of the Board of Directors for any changes in its AML/CFT/CPF policy to remedy any identified weaknesses in the internal controls and risk management practices, should they arise. In alignment with international best practices, senior management oversees the development and implementation of robust employee training programs. These initiatives are designed to enhance staff awareness and understanding of AML/CTF/CPF risks, equipping them especially those in key roles to identify and respond effectively to suspicious activities.

Management also ensures the company's internal control systems are comprehensive and include clear segregation of duties, defined authorization processes, consistent monitoring, and thorough documentation. To reinforce regulatory compliance and optimize the effectiveness of the AML/CTF/CPF program, regular independent audits and evaluations are conducted to provide impartial insights and identify opportunities for improvement.

## **Money Laundering**

Money laundering is an integral part of any financially motivated crime, often on an international scale, such as tax evasion, violations of sanctions, fraud, corruption, illegal arms trade, drug trafficking, extortion, kidnapping etc. Disguising the illegal origin of the criminal proceeds during its processing, including their identity, source and the destination, defines money laundering in broad terms. Therefore, the goal of money laundering is to make the criminal proceeds appear legitimate from the time the money is placed into the financial system ( placement stage), layered in order to hide the audit trail through the web of complex financial transactions at various financial institutions ( the layering stage), to the time it is integrated back into the financial system through the purchase of luxury items or cash intensive businesses (integration stage). Online gambling sites may therefore constitute just one stage of the money laundering process, and this is why it is imperative that casino operators do not offer anonymous services to potential customers and/or facilitate transactions of suspicious nature. Terrorism financing is another “amber alert” for the online operators as the money may move through the system in a similar fashion as the laundered money, despite the fact it often comes from legitimate sources whereas the act is committed for religious or other reasons. Broadly speaking, this refers to the funds that are possessed, used, or received with the purpose of financing acts of terrorism. Prepaid cards have been identified as a highly popular method to acquire materials for the terrorist attacks and therefore it is important to conduct staff training based on newly available information.

## **Key Stages of Money Laundering**

### **Placement:**

The initial stage involves introducing illicit funds into the financial system. Common methods include depositing funds into bank accounts, purchasing high value goods, or conducting other financial transactions. This phase aims to start blending illegal funds into the legitimate economy.

### **Layering:**

In this stage, funds are subjected to a series of complex transactions designed to obscure their origin. Techniques include transferring money across multiple accounts, converting currencies, or investing in financial instruments. The objective is to create a convoluted transaction trail that hinders efforts to trace the funds back to their source.

### **Integration:**

The final stage involves reintroducing the laundered money into the legitimate economy. This is achieved by purchasing luxury assets, investing in cash intensive businesses, or conducting other legal transactions. By this point, the funds appear legitimate, making them more challenging to link to their illicit origins.

Based on the results of the systematic business risk assessments, Aspro N.V.'s main priority is to detect and deter money laundering threats as well as mitigate such risks in the following areas:

- Verification fraud and identity theft (customer due diligence covering documentation verification, age verification and location verification)
- Operation of multiple accounts and high transaction volumes
- Depositing funds obtained from illicit operations and/or using the online platform as “parking”, rather than with the goal of engaging in online gambling or online sports betting.
- Using the online platform as a player-to-player transfer route to funnel funds between sellers and buyers and cashing out when necessary.

This list is not exhaustive and whereas additional risks may materialize from time to time, the Company undertakes to carry out systematic risk assessments tailored to the particular areas of concerns and regular training to its employees with the view of strengthening internal AML compliance programs.

## **Terrorist Financing**

Terrorism-financing is another phenomenon, which covers methods and the means used by terrorist organizations to finance their activities as defined by the United Nations, Office on Drugs and Crime. Countering the financing of terrorism is as important as combating money laundering but its pattern is largely different and is known to comprise small donations from legitimate sources and individuals through charitable organizations or accounts set up at various payment providers. Overall, the FATF (The Financial Action Task Force)

Recommendations 2012/2023 identify customer due diligence, recordkeeping, and reporting suspicious activity as main preventive measures that help businesses combat money laundering. Furthermore, the FATF produced strategic guidance on the AML/CFT/CPF risk-based approach for online casinos where it highlights the vulnerability of online casinos, and gaming sector as regards money laundering (ML) and terrorist financing (TF) risks ( page 59, Vulnerabilities of Casinos and Gaming Sector March 2009) due to the key industry threats associated with the ever evolving techniques of online gambling fraud within the context of limited AML/CFT/CPF controls or regulatory responses in many jurisdictions. From the payment methods standpoint, the volume of remote gambling transactions taking place over the online platforms with 24/7 accessibility is so large and the payment methods are so varied, that it is of paramount importance to develop efficient internal controls based on the periodic reviews of the results of the internal AML/CFT/CPF risk assessments. Notably,

the 2022 Supranational Risk Assessment Report by the European Commission identified the “gambling sector” and online gambling, as a “high risk” area of AML/CFT/CPF concern due to “the no face to face element, huge and complex volumes of transactions and financial flows” involving cryptocurrencies among other payment instruments.

The no exhaustive list of conduct that may be indicative of terrorist financing risk include the following examples:

- The parties to a transaction are based in a country or countries that are on a list of state sponsors of terrorism or a sanctions list.
- Adverse media/ negative news screening reports indicative of links to the terrorist organizations.
- Small regular deposits that are structured to avoid detection.

### **Indicators of Terrorist Financing**

Detecting terrorist financing often involves identifying irregular financial behaviors. Key indicators include:

- Unusual transaction patterns that deviate from established business or personal norms.
- Frequent or large fund transfers linked to high risk regions or known terrorist affiliates.
- Suspicious activities in high risk industries or financial actions that appear designed to obscure terrorist operations.

### **Combating Terrorist Financing**

To counter the risks associated with terrorist financing, Aspro N.V implements robust Anti-Money Laundering (AML) measures, including:

- Customer Due Diligence (CDD): Ensuring thorough verification of customer identities and financial activities.
- Transaction Monitoring: Actively tracking and analyzing financial activities for unusual patterns.
- Sanctions Compliance: Adhering to established sanctions lists to prevent transactions that might inadvertently support terrorism.

Sanctions lists observed by the company include the Sanctions National Ordinance (SNO, N.G. 2014, no. 55), the Kingdom Sanction Act (N.G. 2016, no. 54), and announcements from the Curaçao Gaming Control Board (GCB). Additionally, lists from the Office of Foreign Assets Control (OFAC), United Nations Security Council, European Union, and U.S. List of Foreign Terrorist Organizations are incorporated to ensure comprehensive compliance.

## International Guidelines and Enforcement

Global efforts to combat terrorist financing are supported by:

- Financial Action Task Force (FATF): Setting international standards for identifying and reporting suspicious transactions related to money laundering and terrorist financing.
- Office of Foreign Assets Control (OFAC): Enforcing U.S. economic sanctions and managing the Specially Designated Nationals (SDN) list, which identifies entities involved in terrorism.
- European Union (EU): Mandating member states to implement AML measures and enforce international sanctions to prevent the financial system's misuse.
- United Nations (UN): Imposing sanctions and maintaining lists of individuals and entities linked to terrorism, contributing to global disruption of terrorist funding networks.

## Proliferation Financing

Proliferation financing refers to the financial support provided for the development, acquisition, or production of weapons of mass destruction (WMD), including nuclear, chemical, and biological weapons, as well as their delivery systems. Such financing poses significant risks to global security, and Aspro N.V is fully committed to preventing its involvement in any activities related to proliferation financing. As a licensed casino operator in Curaçao, Aspro N.V adheres to both local regulations established by the Curaçao Gaming Control Board (GCB) and international standards to mitigate risks associated with proliferation financing.

### Sources of proliferation financing

1. **Legal Sources:** Proliferation financing may originate from legitimate business activities, such as trade, investments, or charitable donations, which can be exploited by proliferators to funnel money towards the development of WMDs. Aspro N.V ensures that all transactions, particularly those involving international trade or high risk regions, are subject to thorough scrutiny to prevent misuse in the financing of WMDs.
2. **Illegal Sources:** Similar to other forms of illicit financing, proliferation financing can stem from criminal activities such as smuggling, fraud, and money laundering. Aspro N.V works diligently to identify and prevent any illicit financial activity that may be used to support proliferation related objectives. By maintaining a robust monitoring system, the company aims to detect and disrupt illicit funding sources early in the process.

Funds used for proliferation financing may be transferred through both formal and informal financial channels:

- **Formal Channels:** Financial institutions, including banks and payment processors, are frequently used for proliferation financing. These funds may be layered through complex transactions designed to obscure their origin and destination. Aspro N.V employs advanced transaction monitoring systems to detect suspicious activities, especially when funds are routed through formal banking systems in a manner that appears designed to conceal the purpose of the transaction.
- **Informal Channels:** Informal financial systems, such as trade based financing or alternative remittance networks, can also be exploited for proliferation financing. These systems, operating outside of regulated financial institutions, present a significant challenge to detection. Aspro N.V actively monitors for transactions that may involve high risk jurisdictions or goods that could potentially be used in the development of WMDs, ensuring that all transactions comply with both Curaçao regulations and international sanctions.

Aspro N.V has implemented comprehensive monitoring to detect potential proliferation financing, including the following indicators:

- **Unusual Trade Transactions:** Transactions involving dual use goods items that can be used for both civilian and military purposes are closely monitored. Aspro N.V identifies transactions involving countries or entities linked to proliferation activities, ensuring that trade through the platform does not inadvertently support WMD development.
- **Inconsistent Business Practices:** Aspro N.V remains alert to transactions that appear to lack legitimate business purposes or that are structured in ways designed to evade detection. Suspicious patterns, such as frequent or large transactions that are inconsistent with a customer's normal business activities, are flagged for further review.
- **Suspicious Patterns in Financing:** The company monitors transactions for signs of money laundering or the misdirection of funds intended for legitimate purposes. Transactions involving high risk regions or known proliferators are flagged and investigated for potential involvement in WMD financing.

Aspro N.V employs a robust set of measures to combat proliferation financing:

- **Enhanced Customer Due Diligence (CDD):** Aspro N.V conducts comprehensive customer due diligence (CDD) to verify the identities of its customers, particularly those engaged in international trade or operating in high risk industries. The company ensures that customers and transactions are legitimate, and that there are no links to proliferation financing or activities involving WMDs.

- **Transaction Monitoring:** The company uses state-of-the-art transaction monitoring systems to detect irregular patterns, particularly in high risk transactions. Unusual or suspicious activities, such as large cross border payments, will trigger further scrutiny to ensure that the funds are not being used for illicit purposes, including the financing of WMDs.
- **Sanctions Compliance:** Aspro N.V adheres to both local and international sanctions programs, including those enforced by the United Nations, the European Union, and the U.S. Office of Foreign Assets Control (OFAC). The company ensures that no transactions are conducted with entities or individuals listed on sanctions lists related to the development or proliferation of WMDs.

Aspro N.V follows both local Curaçao regulations and global standards aimed at preventing proliferation financing, including:

- **Curaçao Regulations:** As a licensed casino operator in Curaçao, Aspro N.V adheres to the regulations set forth by the Curaçao Gaming Control Board (GCB) and complies with the relevant national ordinances, including the National Ordinance Penalization of Money Laundering (NOPML) and the National Ordinance on the Reporting of Unusual Transactions (NORUT). These regulations require operators to implement strict Anti-Money laundering (AML) measures to detect and prevent illegal financing, including that related to WMD proliferation.
- **Financial Action Task Force (FATF):** Aspro N.V follows FATF recommendations, which include guidelines for identifying and preventing the misuse of financial systems for proliferation financing. By adopting FATF's recommendations, the company ensures that its compliance program is in line with international best practices.
- **United Nations (UN) and European Union (EU) Sanctions:** Aspro N.V adheres to sanctions lists and regulations issued by the UN, EU, and U.S. OFAC. These sanctions are critical in preventing financial resources from flowing into the hands of entities or individuals involved in the development of WMDs. The company carefully monitors transactions to ensure compliance with these global efforts to curb the proliferation of dangerous weapons.

Through its adherence to local Curaçao regulations and international standards, Aspro N.V ensures that its operations are free from any involvement in the financing of weapons of mass destruction. By employing rigorous monitoring systems, conducting enhanced customer due diligence, and complying with global sanctions, the company actively contributes to global efforts to prevent the spread of WMDs and enhance international security.

## **National Risk Assessment (NRA) Integration**

Aspro N.V maintains a comprehensive AML/CFT/CPF framework designed to prevent its gaming products, services, and platforms from being misused for money laundering, terrorist financing, or proliferation financing. This framework is aligned with Curaçao's legal and regulatory requirements, the expectations of competent authorities, and FATF/CFATF international standards. All employees, management, partners, and service providers are required to follow this framework as part of their operational responsibilities.

The Board of Directors is ultimately responsible for establishing and overseeing an effective AML/CFT program. It ensures that sufficient resources, systems, and qualified personnel are in place to manage the risks associated with online gaming operations. Senior Management supports this oversight by implementing operational controls, ensuring compliance culture, and providing the Compliance Officer with full access to information and systems needed to carry out their duties.

The Compliance Officer is responsible for the day today operation of the AML/CFT program. This includes managing client due diligence, enhanced due diligence, monitoring activities, filing unusual transaction reports, conducting internal investigations, and serving as the primary contact for FIU Curaçao and other supervisory bodies. The Compliance Officer also ensures that internal controls remain aligned with regulatory expectations and national risk developments.

The Company integrates Curaçao's National Risk Assessment (NRA) into its overall risk management framework to ensure it remains aligned with nationally identified threats and vulnerabilities. The Compliance Officer reviews the latest NRA publications and assesses which risks are relevant to the Company's client base, products, payment channels, jurisdictions, and technological environment. The results of this review are incorporated into the Institutional Risk Assessment, which guides the risk-based approach applied across all AML/CFT processes.

Based on the NRA findings, the Company adjusts its internal controls to address high risk areas identified for the gaming sector. These adjustments may include enhanced client verification, increased monitoring thresholds, additional transaction surveillance rules, and restrictions or prohibitions on specific jurisdictions or payment channels. When the NRA identifies new threats, the Company evaluates whether its existing controls are adequate or require strengthening.

Client due diligence is a core component of the Company's AML program. All players must be identified and verified according to the Company's KYC standards before withdrawals or after reaching specified thresholds. Verification includes identity checks, age confirmation, ownership of payment methods, and address verification where applicable. Additional checks are conducted when players trigger risk indicators or engage in high value or unusual patterns.

Enhanced due diligence is applied to clients or activities that pose higher risks. This includes players from high risk jurisdictions, politically exposed persons, high value or VIP players, players involved in complex transaction patterns, and any client whose activity aligns with NRA identified vulnerabilities. EDD may involve obtaining source of funds, source of wealth, adverse media reviews, and approval from Senior Management before continuing the relationship.

Aspro N.V conducts ongoing monitoring of client activity using automated tools and manual oversight. This includes monitoring deposit patterns, bet frequency, wagering behaviour, streak patterns, device data, and potential misuse of bonuses or value transfer schemes. Alerts generated through transaction monitoring systems are reviewed promptly, and suspicious activities are escalated to the Compliance Officer for investigation and reporting if necessary.

All unusual or suspicious transactions identified by the Company must be reported to FIU Curaçao in accordance with NORUT requirements. Internal procedures ensure that employees escalate concerns immediately and maintain confidentiality. Under no circumstances may any staff member inform a player that an internal or external report has been filed, as this constitutes tipping off and is prohibited by law.

Aspro N.V maintains detailed records of all client identification data, verification materials, transaction logs, monitoring results, internal reviews, NRA integration documentation, and FIU reports for a minimum of five years. Regular training ensures that all staff understand AML/CFT obligations, industry specific risks, updated NRA findings, and their individual responsibilities. The AML framework is reviewed annually and updated as needed to remain aligned with regulatory expectations, national risk developments, and technological changes within the gaming industry.

### **Risk Score Calculation**

Money laundering and terrorist financing risks are measured by using a number of factors listed above. Aspro N.V uses the application of risk categories to clients/situations to provide a strategy for managing potential risks and it enables the Company to subject clients to proportionate due diligence and ongoing monitoring. The weight given to these criteria in assessing the overall risk of the client and risk score assigned is as follows:

| Category     | Score                                                   | Level of Due Diligence | Approval process                            |
|--------------|---------------------------------------------------------|------------------------|---------------------------------------------|
| Low Risk     | 02.5                                                    | Standard Due Diligence | Client Service/Compliance Officer           |
| Medium Risk  | 2.53.2                                                  | Standard Due Diligence | Client Service/Compliance Officer           |
| High Risk    | 3.2 or more                                             | Enhanced Due Diligence | Annual and approval from Compliance Officer |
| Unacceptable | Any of the factors that are not accepted by the company | Automatically Reject   | Automatically Reject                        |

The Risk Score correlates with the level of due diligence imposed on the client and who is responsible for conducting due diligence. Regardless of the risk rating, Aspro N.V performs automatic PEP, sanctions and adverse media screening on all clients as part of the client due diligence process and ongoing risk assessment, ensuring the Firm meets its regulatory requirements and obligations.

Further, Aspro N.V uses risk scores in order to determine the different treatments of identification, verification, additional client information, and monitoring for each client as follows:

**Low** – Standard Due Diligence applies. Clients in this category present an overall low risk to the Company, however, because of the high risk nature of online gambling Company will not apply Simplified Due Diligence.

**Medium** – Standard Due Diligence applies. Clients in this category present an overall medium risk to the Company.

**High** – Enhanced Due Diligence applies. Clients in this category present an overall high risk to the Company. These clients will be reviewed by the Compliance Officer and approval or rejection and final signoff. Some of the high risk clients include, but are not limited to:

- the business relationship is conducted in unusual circumstances
- the transaction is complex or unusually large compared to the profile of the client or to other clients of similar type/category
- clients that are resident in geographical areas of higher risk or sanctioned countries
- a client has been identified to be a Politically Exposed Person (“PEP”) or family member or close associate of a PEP. See section on PEPs below.
- clients receive a high risk score at the onboarding stage. See Player Risk Scoring Assessment. **Appendix I.**

- clients that receive high risk scores based on multiple factors described in this procedure (adverse media, a large deposit, and so forth)
- the client has provided false or stolen identification documents or other information on establishing the relationship
- transaction(s) have no apparent economic or legal purpose
- companies that offer financial services or offer services to underlying clients or have underlying clients in any capacity, excluding liquidity providers.
- in combination with other factors, clients with deposit amount over lifetime throughout the entire relationship with the client

### **Unacceptable Clients**

- Person or entities subject to financial sanctions or have been engaged in money laundering activities
- Aspro N.V is required to adhere to the sanction's regime, which is designed to deny services and gambling products to individuals who are deemed to be a high Money Laundering or Terrorist Financing risk. As a result, Aspro N.V is prohibited to enter in any business relationship with individuals or entities listed as targets for financial sanction.
- Individuals under the age of 18 years old. Aspro N.V requires an individual to be at least 18 years old to open an account with the Firm. All individuals under 18 years of age will be automatically rejected.
- Individuals with unknown or unverified wealth sources
- Gameplay matching knows fraudulent patterns

### **ML & TF, PF Risk Assessment**

Company applies a risk based approach in combating exploitation of its online platform for the purposes of ML and TF & CPF. The methodology the Company adopts is based on the Guidance of the Financial Action Task Force (FATF) as regards ML/TF/PF Risk Assessments and determines a risk level by evaluating types of risk, threats, vulnerabilities, controls, consequences, the likelihood of it happening, and the impact it may have on the business model in a particular geographical location. Specifically, AML/CFT/CPF risk assessment categories center around the risks associated.

## **The range of products and services the Company offers**

Online platforms may attract a global clientele, increasing the risk of transactions involving jurisdictions with weak AML controls. Factors that Company considering evaluating Product or Services Risk:

- The complexity of the product, service, or transaction
- The value or size of the product, service, or transaction
- Services provided through third party providers or affiliates (e.g., payment processors, game providers) add an additional layer of risk.

### **Low to Medium Risk**

- EEA countries.
- Third countries with effective mechanisms to combat money laundering and financing of terrorism.
- Third countries, which credible sources have identified as countries with a limited extent of corruption or other criminal activity.
- Third countries which, based on credible sources such as mutual evaluations, reports on detailed assessment or publicly available follow-up reports, have requirements to combat money laundering and financing of terrorism which are consistent with the FATF recommendations and which implement these requirements in an efficient manner.

### **High to Ultrahigh Risk**

- Countries which do not have effective mechanisms to combat money laundering and financing of terrorism.
- Countries, which credible sources have identified as countries with a significant level of corruption or other criminal activity.
- Countries subject to sanctions, embargoes, or similar measures taken by, for example, the EU or UN; o Countries that finance or support terrorist activities, or which house known terrorist organizations.

## **Adherence to Curaçao's Updated Legislative Framework**

Aspro N.V aligns its practices with the revised LOK framework, ensuring compliance with all AML/CTF/CPF requirements. The company's compliance program incorporates a robust risk-based approach tailored to its operational scope and complexity. Regular training sessions are provided to staff, ensuring that they understand their AML/CTF/CPF obligations and how to manage risks effectively. Independent audits are carried out periodically to assess the performance and effectiveness of the company's AML/CTF/CPF strategies and the application of the risk-based approach.

Aspro N.V recognizes the unique risks posed by the gambling sector, particularly in relation to money laundering and terrorist financing. The company identifies and mitigates customer risks by conducting comprehensive customer due diligence (CDD) and enhanced due diligence (EDD) for high risk individuals. Key customer risk factors include irregular income sources, high spenders, and PEPs. Continuous monitoring and profile updates, along with stringent identity verification, are employed to mitigate these risks.

### **Customer Risk**

The company evaluates customer risk by examining factors that could indicate a heightened likelihood of involvement in financial crime. This includes assessing the customer's financial behavior, the transparency of income sources, and potential affiliations with politically exposed persons (PEPs). Customers with multiple or opaque income streams, or those demonstrating inconsistent or high volume financial activity that is not aligned with their declared profile, are considered higher risk and subjected to enhanced due diligence (EDD).

Clients who maintain multiple accounts or who exhibit spending patterns that significantly exceed their known financial means may attempt to obscure transaction trails, which complicates compliance efforts. Aspro N.V sets clear transaction thresholds based on typical user behavior to trigger investigative reviews. Low risk customers generally have a single, documented source of income and a consistent transactional footprint, while higher risk individuals are flagged for closer scrutiny, including more rigorous KYC documentation and monitoring protocols.

### **Risk Based Approach (ML/ TF risks' detection)**

Company applies a risk-based approach in combating exploitation of its online platform for the purposes of ML and TF. The methodology the Company adopts is based on the Guidance of the Financial Action Task Force (FATF) as regards ML/ TF Risk Assessments and determines a risk level by evaluating types of risk, threats, vulnerabilities, controls, consequences, the likelihood of it happening, and the impact it may have on the business model in a particular geographical location.

Aspro N.V. conducts a formal Business Risk Assessment (BRA) annually and upon any significant operational change. This BRA evaluates money laundering and terrorism financing risks associated with clients, products, delivery channels, geographical exposure, and technological developments. The assessment is documented, approved by the Board of Directors, and revised in accordance with the latest regulatory updates or business model changes

Specifically, AML/CFT risk assessment categories center around the risks associated with:

### **Risk Factors**

Client risk pertains to the likelihood of exposure to money laundering (ML) and terrorism financing (TF) through interactions with particular individuals. As part of its risk-based compliance model, Aspro N.V. conducts thorough evaluations of client profiles, financial transactions, and sources of wealth to identify potential vulnerabilities.

Certain client types are considered to carry a higher risk of financial crime involvement. This includes individuals with multiple income streams, which can complicate the verification process of fund legitimacy. Clients with fluctuating or unpredictable financial behavior may also increase the risk due to the challenge in assessing their financial patterns. Politically Exposed Persons (PEPs) are subject to intensified scrutiny owing to their potential influence over public funds and associated corruption risks.

Additional high risk categories include individuals with substantial and inconsistent spending, whose expenditures appear disproportionate to their declared income, and clients who maintain multiple gaming accounts, potentially to evade monitoring or obscure financial activity. To address these risks, Aspro N.V. has implemented transaction thresholds that reflect normal client behavior patterns.

Typically, lowrisk individuals are characterized by having a single, verifiable source of income. In contrast, those with multiple income sources, inconsistent spending patterns, or irregular transactions are subject to elevated monitoring and Enhanced Due Diligence (EDD) measures.

### **Transactional Risk Exposure**

Certain products and transaction types within the iGaming and digital services sector are more prone to misuse for illicit purposes. Services that allow rapid, high volume transactions or offer anonymity such as the use of cryptocurrencies or prepaid instruments can be exploited to introduce, layer, and integrate proceeds from criminal activities into the legitimate financial system.

Examples of heightened product and transaction risks include:

- Use of gaming or wallet accounts primarily as passthrough mechanisms without active service usage.
- Peer to peer fund transfers that bypass conventional financial monitoring systems.
- Deposits or withdrawals made using third party financial tools, including bank accounts or cards not registered to the account holder.

### **Geographical Risk Considerations**

Geographic risk is assessed by evaluating the customer's country of residence or the origin of their financial resources. Certain jurisdictions are associated with weak AML/CTF enforcement, high levels of public corruption, or a history of noncooperation with international regulatory bodies. Engagement with clients or transactions linked to these jurisdictions poses an elevated compliance concern.

Aspro N.V relies on guidance from internationally recognized bodies to evaluate and respond to geographic risks, including:

- FATF list of jurisdictions under increased monitoring or subject to countermeasures.
- Regional reports from the Caribbean Financial Action Task Force (CFATF).
- U.S. State Department International Narcotics Control Strategy Reports (INCSR).
- The European Commission's list of high risk third countries.
- OFAC sanctions databases and the Transparency International Corruption Perceptions Index (CPI).

To counter these risks, Aspro N.V monitors all platform based transactions in real time and uses automated detection systems to flag atypical behavior. Where red flags are identified, the company initiates investigative protocols and applies EDD measures to assess potential threats.

Based on these sources, the company categorizes countries into varying levels of risk. Clients from high risk jurisdictions are subjected to strict onboarding controls and enhanced monitoring, while transactions involving sanctioned countries are blocked or escalated for additional review. Geographical risk profiles are revisited regularly to ensure the company's controls remain responsive to global developments.

### **Distribution Channel Risk and Authentication Controls**

The methods through which Aspro N.V establishes and manages customer relationships also influence its exposure to financial crime. Channels that permit remote or anonymous access, especially without sufficient verification layers, are inherently more susceptible to misuse. This is particularly relevant in digital environments where face-to-face interaction is absent.

To reduce this risk, the company employs secure identity verification protocols for all customers. These include biometric checks, multifactor authentication, and identity validation tools that interface with global databases. By ensuring that access to services is tightly controlled and all interactions are traceable, Aspro N.V maintains operational integrity and regulatory compliance.

### **Technological Developments Risk Assessment**

Prior to the launch of any new technology, digital product, delivery method, or operational process, Aspro N.V. conducts a formal and documented technological risk assessment. This process is mandatory and forms a core component of the Company's risk-based approach to AML/CTF/CPF compliance.

The risk assessment must be:

- Completed and reviewed prior to deployment, ensuring no new technology is introduced without first understanding its vulnerabilities and potential misuse.
- Fully documented in writing, including details of the product or system being assessed, identified risks, mitigation measures, residual risk levels, and decision-making rationale.
- Retained in internal compliance records and made available to the Curaçao Gaming Control Board (GCB) upon request.

Documented assessments are required for:

- New gaming platforms, digital tools, or payment channels.
- Any update to existing infrastructure that significantly changes risk exposure.
- The use or integration of AI systems, blockchain, or third party services.
- Innovations involving anonymous payment mechanisms or remote account access.

This approach ensures all technological advancements are introduced responsibly, with due consideration for AML/CTF/CPF risks and are aligned with the supervisory expectations of the GCB.

Aspro N.V. is dedicated to ensuring that advancements in technology are not exploited for the purpose of financial crimes such as money laundering (ML) or terrorist financing (TF). As innovation continues to transform the iGaming sector, the company implements robust controls and a proactive risk management framework to identify and mitigate any vulnerabilities associated with technological change. Through the integration of thorough risk evaluation processes, Aspro N.V. safeguards its compliance obligations across all new business practices, service models, and product innovations.

#### Procedures for Risk Identification and Assessment

In order to detect and manage risks associated with technological innovation, Aspro N.V. conducts in-depth assessments in the following scenarios:

- The launch of a new product or feature on the gaming platform;
- The introduction of operational practices aimed at improving efficiency or enhancing user engagement;
- The adoption of novel service delivery mechanisms, including modern payment technologies or digital account access tools;
- The deployment or integration of emerging technologies into current or future gaming infrastructure, such as blockchain solutions, Ai powered services, or advanced cybersecurity protocols.

Prior to implementing any new technology, a comprehensive review is conducted to assess potential vulnerabilities that could be exploited for criminal activity. This process involves identifying and analyzing associated risks and ensuring all findings are thoroughly documented. The assessment is aligned with both domestic and international AML/CTF regulatory frameworks, reinforcing the company's ability to identify, manage, and mitigate technology driven threats related to financial crime.

### **Implementation of Mitigation Strategies**

Upon identification of potential risks, Aspro N.V. promptly adopts appropriate mitigation measures to reinforce its defenses against emerging threats. These may include:

- Strengthening of Security Protocols – The implementation of multifactor authentication (MFA), biometric identity verification, end to end data encryption, and artificial intelligence (AI)based fraud detection tools to safeguard systems from misuse;
- Enhancement of Transaction Monitoring Capabilities – Upgrading monitoring platforms to detect atypical financial behavior using automated systems capable of flagging transaction patterns indicative of ML or TF;
- Policy Adaptation – Revising AML/CTF policies to address new risk factors introduced by evolving technology. The company ensures that its compliance framework remains agile, keeping pace with the dynamic nature of cybercrime and financial crime techniques.

Through ongoing monitoring and adjustment to technological developments, Aspro N.V. upholds its commitment to maintaining a secure and compliant operational environment. This forward-looking strategy protects the integrity of the company's financial ecosystem and affirms its alignment with global AML/CTF obligations. By doing so, the company ensures that innovation is not pursued at the expense of regulatory compliance or financial security.

Based on the analysis of the risk indicators, the risk model calculates a risk rating of low, medium or high which is then used to create a risk profile which is then assigned to the players and payment service providers at the onboarding stage and is reassessed and amended during the business relationship within the framework of periodic KYC/KYB reviews. Online casinos possess inherent high risks, so the Company strives to rely on its AML and Antifraud key personnel to maintain effective internal controls and CDD measures as reflected in relevant policies

Key mitigation measures include:

- **Strengthening security infrastructure**, such as deploying multifactor authentication (MFA), biometric identification, advanced data encryption, and AIbased fraud detection technologies.
- **Enhancing monitoring capabilities**, ensuring that transaction surveillance systems can detect and escalate anomalies in real time especially those reflecting structuring, layering, or uncharacteristic activity patterns.

- **Adapting compliance policies** to reflect the risks posed by digital transformation. The AML/CTF framework is updated regularly to account for emerging crime methodologies and to incorporate new risk indicators tied to technological abuse.

### **Commitment to Secure Innovation**

Aspro N.V is committed to fostering innovation in a manner that reinforces not undermines its compliance posture. The company's approach to technological adoption emphasizes anticipation of risk, continuous system evaluation, and robust internal governance. Regular reviews of deployed technologies are conducted to reassess vulnerabilities and to adapt mitigation measures as necessary.

By incorporating these risk-based strategies into its AML/CTF/CPF policy, Aspro N.V effectively mitigates the risks associated with money laundering, terrorist financing, and proliferation financing. The company is committed to upholding Curaçao's regulatory standards while ensuring the integrity and security of the gaming sector.

Based on the analysis of the risk indicators, the risk model calculates a risk rating of low, medium, or high which is then used to create a risk profile which is then assigned to the players and payment service providers at the onboarding stage and is reassessed and amended during the business relationship within the framework of periodic KYC/KYB reviews. Online casinos possess inherent high risks, so the Company strives to rely on its AML and Antifraud key personnel to maintain effective internal controls and CDD measures as reflected in relevant policies.

## **Compliance Officer**

Compliance officer oversees the AML compliance program, i.e., actively manages money laundering, terrorist financing and proliferation financing risks. It is a crucial role which encompasses being authorized to communicate with the regulatory bodies, supervision of a team of internal compliance officers and their day to day operations, including maintaining robust age verification protocols, promoting responsible gambling practices, preventing gambling related addiction, promoting self exclusion tools, and maintaining a watchful eye over all due diligence and antifraud procedures with the view of conducting regular risk assessments. The Officer is also responsible for reporting suspicious activity, including suspicious transactions, to the FIU in Curacao.

Internally, the Compliance Officer is requested to report to the Board of Directors to keep the Board members informed of any recommended changes that may be required to manage the AML/CFT/CPF compliance program.

The compliance officer is assigned the following responsibilities (list is not exhaustive)

- To design and implement the AML program.
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing.
- To review compliance with the casino's policy and procedures.
- To organize training sessions for the staff on various compliance related issues.
- To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions.
- To review all internally reported unusual transactions for their completeness and accuracy with other sources.
- To keep records of internally and externally reported unusual transactions.
- To execute closer investigation of unusual transactions if necessary.
- To prepare the external report of unusual transactions.
- To make necessary changes to the AML program.
- To remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements.
- To prepare periodic information on the casino's efforts against money laundering and financing of terrorism and financing of proliferation.

The AML/CFT/CPF Officer acts independently always and his/her decision making process is not impeded by the operational goals of the Company when investigating internal or external reports of suspicious activity.

As part of combating money laundering, fraud and terrorist financing, players' IP addresses are tracked via an embedded tool in the proprietary antifraud system to ensure the site is accessed from nonrestricted countries. This measure also helps detect suspicious activity such as attempts to set up multiple accounts by the same individual, or block individuals who have been blacklisted or self excluded. The proprietary software also monitors data as regards the players' transaction history, betting amount, information on wins and losses, players' geolocation, pattern of gambling activity and duration of playing. These tools may be used in instances where a customer risk's rating is deemed to be high due to presence of some behavioral or transactional triggers that point to a potential AML/CFT/CPF breach.

### **Customer Due Diligence Guidelines**

The Company does not accept or maintain anonymous accounts under fictitious names. Aspro N.V. does identify each player/client, gathering its name and other relevant information to understand the purpose and nature of the business relationship. Without adequate knowledge of the customer, the Company does not establish nor maintain a business relationship, nor process occasional transactions. When establishing a business relationship with customers the Company identifies whether a customer wishing to use the Company's online platform poses any money laundering, terrorist financing or proliferation financing threats to its ecosystem. CDD forms the basis of the risk-based assessment for risk scoring purposes. In the context of AML, customer due diligence process is a procedure which includes the identification of the potential customer, verification of his/her identity and age, collection of additional information to construct an economic profile of the account holder, assign a risk rating and monitor his behavioral and transactional patterns for any deviations that may be construed as a violation of AML/CFT/CPF legislation and policies. Research into the customers can be done via opensource tools such as social media checks, property ownership checks, employment checks, insolvency checks etc. Due Diligence measures may be simplified when the analysis of the initial customer data places such applications in a low risk category, whereas Enhanced Due Diligence is applied to cases that require additional screening due to the system flagging certain data entries.

Transactions of NAF 4,000 or more: CDD measures are applied to any single transaction that meets or exceeds this threshold.

Occasional transactions exceed NAF 4,000: This includes infrequent transactions that surpass the specified limit.

Suspicion of illicit activities: Any indication of money laundering or terrorist financing will trigger CDD protocols.

Uncertainties in client identification: If previously obtained identification data raises doubts, CDD measures will be activated.

Linked transactions: This applies to either a single transaction or multiple transactions that collectively exceed NAF 4,000. Even if individual transactions are below this threshold, linked transactions will still necessitate CDD. High risk transactions will require Enhanced Due Diligence (EDD).

The company's CDD procedures will encompass the following actions:

Identity Verification: Players will be identified using credible, independent documents or data. This process includes confirming the ultimate beneficial owner of legal entities and understanding their ownership structure.

Ongoing Monitoring: Continuous due diligence will be conducted to monitor transactions, ensuring alignment with the company's understanding of the player and their risk profile, including the source of funds as needed.

Confidential Reporting: Employees are instructed to maintain confidentiality regarding reports made to the FIU, thereby preventing players from being alerted. If suspicions of money laundering or terrorist financing arise, the company will bypass standard CDD processes and report directly to the FIU.

**To establish a player's identity, the following information will be collected:**

- Full name
- Permanent residential address
- Date of birth
- Place of birth
- Nationality
- Identity number
- For low risk scenarios, only basic information will be required. In high risk situations, more detailed information will be collected to mitigate the risks associated with money laundering and terrorist financing.
- Risk Evaluation: Players will be assigned initial risk ratings based on collected information, which will be revised as more data becomes available to determine the appropriate level of CDD.
- Verification Methods: Identity verification will be executed through:
  - Government issued photo identification (e.g., passport or ID card).
  - Supplementary documents (e.g., utility bills or bank statements) confirming the address, dated within the last six months.

- Verification of the address through communication methods such as letters, email, or phone.
- Biometric checks, cross referencing database information, IP addresses, and funding methods.
- If initial information is insufficient, further verification steps may include requesting a selfie with the ID or confirming the first deposit through a regulated financial institution.

The company will seek to identify the purpose and nature of its relationships with players as part of the CDD process. While some relationships may be clear, the company will gather sufficient information to detect any unusual or suspicious activities. For higher risk

clients, detailed documentation of their source of wealth and expected activity levels will be collected to ensure legitimacy. For lower and medium risk players, basic employment or business information will suffice, supplemented by independent verification for higher risk individuals.

### **Timing of Client Due Diligence Measures**

Aspro N.V. enforces the timely implementation of Client Due Diligence (CDD) procedures to ensure full compliance with applicable Anti-Money Laundering (AML), Counter Terrorist Financing (CTF), and Counter Proliferation Financing (CPF) regulations. These procedures are designed to proactively identify and verify clients in accordance with regulatory requirements and internal risk assessments.

#### **CDD Triggered by Transaction Thresholds**

At the point of account registration, Aspro N.V. collects and verifies core client information, including full legal name, permanent residential address, and date of birth. Additionally, clients undergo Politically Exposed Person (PEP) screening and are crosschecked against relevant sanctions lists to ensure they are not linked to prohibited or high risk entities.

In line with the company's risk-based approach, full identity verification is completed prior to processing any financial transaction that reaches or exceeds the threshold of NAF 4,000. This requirement applies to both individual transactions and cumulative transactions such as multiple deposits, withdrawals, or player to player transfers that collectively meet the threshold within a relevant time frame.

Aspro N.V. actively monitors all financial activity on a continuous basis. Transaction data is aggregated daily to ensure that the cumulative behavior of each player is considered when assessing risk exposure and determining the need for additional due diligence.

When the threshold of NAF 4,000 is met, the company conducts a comprehensive client risk assessment. This includes reviewing all previously collected information, completing any outstanding CDD obligations, and updating the client's risk classification as needed.

#### **Early Execution of CDD Procedures**

As a proactive measure, Aspro N.V. aims to complete CDD procedures at the earliest opportunity preferably during account registration regardless of whether a financial threshold has been reached. By verifying client identities prior to their participation in financial transactions, the company reduces the likelihood of criminal actors exploiting the platform before thorough due diligence has been conducted

#### **Temporary Restrictions for Incomplete CDD**

In circumstances where a client reaches the NAF 4,000 threshold before completing full CDD verification, Aspro N.V. applies specific transactional restrictions to preserve regulatory compliance:

If the threshold is met due to a deposit, the client is prevented from making further deposits or withdrawals. However, they may continue using existing funds for gameplay activities.

If the threshold is reached due to a withdrawal request, the client's account is temporarily frozen, and all gaming activity is suspended until the verification process has been finalized.

#### **Addressing CDD Noncompliance**

If a client fails to submit the required CDD documentation within 30 days of reaching the NAF 4,000 threshold, Aspro N.V. initiates corrective action. The business relationship is terminated, and depending on the circumstances, the company takes the following steps:

If the situation gives rise to a reasonable suspicion of ML or TF, a Suspicious Transaction Report (STR) is submitted to the Financial Intelligence Unit (FIU).

In the absence of such suspicion, the remaining funds are returned to the original deposit source (e.g., the client's verified bank account or digital wallet).

If there are lingering concerns about possible financial crime, the company evaluates whether the funds should be frozen in accordance with its internal escalation procedures and regulatory requirements.

#### **Preventing Tipping Off**

Aspro N.V. is mindful of the risks associated with tipping off a client during account restriction or closure. In such cases, the company ensures that all actions are carried out discreetly and in accordance with legal obligations. Staff are guided by internal procedures designed to avoid breaching anti-tipping off provisions while maintaining full regulatory compliance.

By ensuring that CDD measures are implemented swiftly and in alignment with financial activity thresholds, Aspro N.V. strengthens its defences against financial crime, upholds transparency, and safeguards the integrity of its gaming platform across all operational channels.

### **Continuous Surveillance of Existing Clients**

Aspro N.V. applies Client Due Diligence (CDD) not only at the onboarding stage but also throughout the duration of the client relationship. The company is committed to maintaining a high standard of compliance by performing ongoing monitoring and routine reassessments, ensuring that all client activity remains consistent with prevailing Anti-Money Laundering (AML), Counterterrorism Financing (CTF), and Counter Proliferation Financing (CPF) regulations.

### **Ongoing Review and Risk-based Monitoring**

Client relationships are subject to continuous due diligence measures. This includes the regular monitoring of transactions and the reassessment of client risk profiles in light of new behaviors or patterns. Where necessary, the company reevaluates previously collected data to ensure it remains accurate, complete, and relevant. Any deviation from expected conduct prompts further review and, where applicable, the application of enhanced scrutiny.

For clients who were previously onboarded with limited or incomplete CDD, Aspro N.V. initiates retrospective due diligence procedures. These are prioritized based on risk, with high risk clients undergoing immediate verification. Periodic updates are also conducted in accordance with both internal policies and regulatory guidance to ensure that CDD measures remain aligned with risk exposure and evolving compliance standards.

### **Reapplication of CDD Based on Risk Triggers**

Aspro N.V. applies full CDD measures to existing clients under specific conditions that indicate increased risk or regulatory necessity. These conditions include, but are not limited to:

A material change in the client's behavior or risk profile, such as sudden high value transactions, relocation to a higher risk jurisdiction, or being identified as a Politically Exposed Person (PEP).

Legislative or regulatory amendments that require updated or additional client verification.

The client engaging in one or more transactions totalling NAF 4,000 or more, which automatically triggers full identity verification and documentation review under the company's CDD policy.

### **Remediating Gaps in Historical CDD**

In instances where clients were previously allowed to transact without complete CDD such as during legacy onboarding procedures or prior to the implementation of current regulatory standards Aspro N.V. takes corrective action. High risk clients are prioritized for immediate verification, while others are subject to a scheduled review based on the level of risk they present.

CDD is applied using a proportional and risk sensitive approach, ensuring that resources are allocated where they are most needed and that lower risk clients are still monitored effectively. Verification processes may include updated identity checks, refreshed PEP and sanctions screenings, and a reassessment of the client's source of funds and wealth.

By extending due diligence practices beyond initial onboarding and embedding them into the ongoing management of client relationships, Aspro N.V. strengthens its regulatory compliance, reduces its exposure to financial crime, and upholds the integrity of its platform across all client segments.

### **Termination of Business Relationships**

Aspro N.V. maintains the right to terminate business relationships with clients who fail to comply with Client Due Diligence (CDD) requirements or who present heightened financial crime risks. This measure ensures the company's adherence to Anti-Money Laundering (AML), Counterterrorism Financing (CTF), and Counter Proliferation Financing (CPF) regulations while preserving the security and integrity of its operations. Business relationships are subject to termination when a client engages in suspicious or unexplained financial activities, fails to submit required CDD documentation within the prescribed timeframe, or is determined to pose a significant risk of involvement in money laundering or terrorist financing. The decision to terminate a relationship is subject to formal internal review and must be approved by senior management.

Prior to termination, a final review of the client's account activity is conducted to identify any outstanding irregularities. If any transaction raises suspicion of ML, TF, or PF Aspro N.V. submits a Suspicious Transaction Report (STR) to the Financial Intelligence Unit (FIU) without delay. All records associated with the terminated relationship are retained securely for a minimum of five years in accordance with regulatory requirements. This approach reinforces the company's commitment to proactive risk management and ensures regulatory compliance through the entire client lifecycle.

Where risk cannot be adequately mitigated such as uncooperative clients, unresolved discrepancies, or confirmed links to sanctioned entities Aspro N.V. will terminate the business relationship and report such instances to the Financial Intelligence Unit (FIU)

### **Third party Reliance for Client Due Diligence**

Aspro N.V. may, under controlled circumstances, rely on qualified third parties to carry out specific components of the Client Due Diligence (CDD) process. Such reliance is implemented strictly within the boundaries of applicable AML/CTF/CPF laws and does not absolve the company of its legal responsibility to ensure full compliance. Aspro N.V. remains ultimately accountable for the accuracy, completeness, and timeliness of all CDD related activities performed on its behalf.

When relying on a third party, the company ensures that all relevant client identification and verification information is accessible without delay upon request. Third party arrangements are governed by formal agreements that clearly outline data sharing protocols, compliance obligations, and procedures for independent compliance audits. These agreements require the third party to be a regulated entity subject to robust AML/CFT supervision and to maintain an independent relationship with the client.

Importantly, Aspro N.V. differentiates between third party reliance and outsourcing. In a reliance scenario, the external party performs selected CDD tasks independently, while Aspro N.V. retains full responsibility for assessing client risk, verifying Politically Exposed Person (PEP) status, and maintaining ongoing transaction monitoring. In an outsourcing arrangement, the third party operates under Aspro N.V.'s direct oversight, following its internal policies and regulatory framework.

Before engaging with any third-party service provider, Aspro N.V. conducts a comprehensive risk assessment of the provider's jurisdiction, evaluating its regulatory environment and compliance history. This is supported by intelligence from international

watchdogs and enforcement bodies. Regular assessments both quantitative and qualitative are performed to monitor the third party's performance and ensure the effectiveness of their procedures. These reviews verify that decisions regarding business relationships and risk classification remain under the exclusive control of Aspro N.V.

Through structured oversight and stringent regulatory controls, Aspro N.V. ensures that any third-party involvement in CDD processes contributes to a secure, transparent, and compliant operational environment.

### **Beneficial Ownership Identification and Control Structure Verification**

Aspro N.V. undertakes all reasonable measures to identify, verify, and understand the Ultimate Beneficial Owners (UBOs) and the ownership and control structures of legal entity clients, in full compliance with AML Regulation III.2.2 and relevant international best practices.

This obligation extends beyond basic identification of beneficial owners and requires a full understanding of how ownership and control are exercised within the customer's structure, both onboarding and throughout the course of the business relationship.

To meet this obligation, Aspro N.V. applies the following measures:

- Identify and verify natural persons who ultimately own or control 25% or more of the equity, voting rights, or capital of a legal entity, whether directly or indirectly.
- Where no individual meets the ownership threshold, identify any persons who otherwise exercise effective control, such as through:
  - Voting arrangements, contractual relationships, or positions of influence (e.g., board control or management power).
  - Indirect control mechanisms, such as trusts, nominee arrangements, bearer shares, or layered ownership through multiple legal entities.
- Conduct multitiered analysis in cases where ownership is obscured through multiple corporate layers or complex holding structures, to trace and identify the natural person(s) exercising ultimate control.
- Obtain and review reliable documentation such as:
  - Shareholder registries, articles of incorporation, beneficial ownership registers.
  - Declarations from legal representatives clarifying control and ownership hierarchy.
  - Organizational charts and financial disclosures when necessary.
- Where no individual qualifies under the above, identify the most senior managing official as a fallback UBO, in accordance with the “last resort” principle under FATF and CGA guidance.
- Verify beneficial ownership and control details using independent and reliable sources, and ensure this information is:
  - Accurately recorded and readily available for competent authorities.
  - Regularly reviewed and updated, particularly when:
    - There is a change in ownership or control.
    - The customer’s risk profile changes.
    - Trigger events occur (e.g., threshold transactions, suspicious activity).

Aspro N.V. does not enter or continue business relationships with legal entities whose beneficial ownership or control structures are nontransparent, unverifiable, or otherwise obstructive to due diligence.

The integrity of the gaming environment is maintained through the application of protocols based on utilizing advanced technology and third party databases including a proprietary antifraud system for onboarding and transaction monitoring, artificial intelligence tools (AI), biometric identification in some instances and RegTech screening tools such as WorldCheck, LexisNexis, SEON etc. Activities or type of players that may indicate a higher risk include the following categories:

1. Anonymous customers
2. Economic profile is inconsistent with the increase in gambling activity
3. Requests to withdraw winning via another payment method which differs from the one that was used for the original placement of the bet.
4. Attempts by the same individual to create multiple accounts
5. Drastic changes in the gambling pattern
6. High value staking/ high transaction volume
7. Unusual requests that do not fall within the recommended guidelines such as to bypass KYC verification process etc.

Antifraud team oversees operating a proprietary system which analyzes players' data based on the automatic checks performed through several third party databases such as World Check, Dow Jones and Lexis Nexis. In addition, manual checks are performed by a team of analysts via various data sources. Any discrepancies identified by the first line of defense are escalated to the team lead and then may be ultimately reported to the Compliance Officer in writing through an internal suspicious activity report (SAR).

**Customer Due Diligence** is triggered in the following scenarios:

- When identifying the player and verifying that customer's identity using reliable, independent source documents, data or information.
- When identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner. For legal persons and legal arrangements, the Company seeks to understand the ownership and control structure of the customer.
- If suspicions are raised as regards the authenticity of the information and documents obtained during the onboarding process.
- If there is a suspicion of money laundering or terrorist financing as regards the customer's profile and activity.
- If there are any unauthorized changes detected as regards the player's profile.
- When transactions of NAF 4,000 or more appear CDD measures are applied to any single transaction that meets or exceeds this threshold.
- When occasional transactions exceeding NAF 4, 000 CDD measures are applied. This includes infrequent transactions that surpass the specified limit.
- When to either a single transaction or multiple transactions that collectively exceed NAF 4,000 appear CDD measures are applied. Even if individual transactions are below this threshold, linked transactions will still necessitate CDD.
- Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

The wagering of a stake, the deposit of funds or the collection of the winnings through the withdrawal of the funds constitute a transaction in such cases.

Periodic reviews of the existing records and ongoing monitoring of the transactional patterns of the regular players also form an integral part of the CDD measures.

In cases where the CDD measures cannot be applied, the account gets locked during an attempt to complete CDD and ultimately the business relationship with the customer gets terminated due to the failure to satisfy AML/ CFT legislative requirements and the funds are refunded back to the customer through the same payment channel and account used to deposit the funds.

### **Player Identity Establishment**

To establish a player's identity, Company collects the following information:

- Full name
- Permanent residential address
- Date of birth
- Place of birth
- Nationality
- Identity number

For low risk scenarios, only basic information will be required. In high risk situations, more detailed information will be collected to mitigate the risks associated with money laundering and terrorist financing.

**Risk Evaluation:** Players will be assigned initial risk ratings based on collected information, which will be revised as more data becomes available to determine the appropriate level of CDD.

**Verification Methods:** Identity verification will be executed through:

- Government issued photo identification (e.g., passport or ID card).
- Supplementary documents (e.g., utility bills or bank statements) confirming the address, dated within the last six months.
- Verification of the address through communication methods such as letters, email, or phone.
- Biometric checks, cross referencing database information, IP addresses, and funding methods.

If initial information is insufficient, further verification steps may include requesting a selfie with the ID or confirming the first deposit through a regulated financial institution.

The company reserves the right to terminate relationships with players engaged in suspicious activities or those who fail to provide sufficient information. Such decisions must be documented and approved by senior management. Upon termination, all activities will be reviewed, and any suspicious transactions will be reported to the FIU. Records related to terminated relationships will be securely stored for a minimum of five years.

### **Timing of Customer Due Diligence Measures**

Aspro N.V applies Customer Due Diligence (CDD) measures in a timely and systematic manner, in line with its regulatory obligations under Anti-Money Laundering (AML), Counter Terrorism Financing (CTF), and Counter Proliferation Financing (CPF) frameworks. These procedures are designed to ensure that customer identification, verification, and risk assessment occur at the appropriate stages of the business relationship and in response to specific financial thresholds or behavioral indicators.

### **CDD Triggers Based on Transaction Thresholds**

Upon account registration, the company collects the following minimum customer data:

- Full legal name
- Permanent residential address
- Date of birth
- Politically Exposed Person (PEP) status screening
- Sanctions screening against relevant domestic and international lists

As part of its risk-based methodology, Aspro N.V ensures that identity verification is completed before the execution of any transaction (or linked series of transactions) equal to or exceeding NAF 4,000.

This threshold based verification applies to:

- A single transaction that reaches or surpasses the NAF 4,000 limit.
- Multiple linked transactions including deposits, withdrawals, and peer to peer transfers that cumulatively meet or exceed this value.

To ensure full regulatory compliance, the company monitors transaction activity on a daily rolling basis, calculating total exposure from the start of the customer relationship. Once the NAF 4,000 threshold is triggered, Aspro N.V immediately conducts a full risk assessment and completes any outstanding due diligence requirements before allowing further financial activity.

## **Transaction Monitoring**

Transaction monitoring in the betting and gambling industries is a critical component of regulatory compliance and Anti-Money laundering (AML) efforts. Given the high volume of transactions and the potential for misuse, these industries are closely monitored by regulatory bodies to prevent illicit activities such as money laundering, fraud, and financing of terrorism. Aspro N.V.'s objective is to mitigate challenges arising from the high volume and velocity of transactions where makes challenging to monitor each transaction effectively, and the use of cryptocurrencies and other digital payment methods that complicate the monitoring process.

In a nutshell, the Curacao regulatory landscape focuses on defining the indicators that may suggest the transaction is of an unusual nature so that it may be reported to the Curacao Financial Intelligence Unit (FIU Curacao). Therefore, an adequate transaction monitoring system is a vital part of complying with the licensing requirements in Curacao.

Aspro N.V.'s antifraud team is in charge of operating a proprietary antifraud system which analyzes players' data on the basis of the automatic checks performed through a number of electronic systems such as WorldCheck and manual checks performed by a team of analysts via various data sources. Any discrepancies identified by the first line of defense are escalated to the team lead and then may be ultimately reported to the AML/CFT Officer in writing through an internal suspicious activity report (SAR).

This system is an automated monitoring system which allows to monitor transactions in real time, flagging suspicious activities based on predefined rules and thresholds. The anti fraud team uses machine learning and data analytics to enhance detection capabilities and reduce false positives. Additionally, the system is configured in a such a way as to focus on high risk transactions, such as large deposits, frequent transfers, and cross border transactions and the parameters reflect current and emerging threats to capture bad actors by flagging suspicious activity internally, and, where necessary, to financial intelligence units (FIUs).

### **Components of transaction monitoring system**

**Automated System:** Advanced software solutions are employed to monitor transactions in real time. These systems use algorithms and machine learning to identify patterns and anomalies that may indicate suspicious activities.

**Risk Assessment:** clients and transactions are assessed for risk based on various factors, including the amount and frequency of transactions, geographic location, and client behavior.

**Alert Generation:** When suspicious activity is detected, the system generates alerts that are reviewed by Compliance Officer. Alerts are based on predefined rules and thresholds, such as unusually large transactions or frequent deposits and withdrawals.

Common techniques include geolocation tracking, source of funds verification for high value transactions, behavioral analysis by monitoring changes in betting patterns or gambling behavior that deviate from the norm for a specific client as well as transaction velocity (quick movement of funds between accounts and/or frequent high value transactions within a short period).

CDD is triggered in the following scenarios: creation of an online account; doubts about the authenticity of the provided information and documents; suspicious client profile and/or transactional activity, unauthorized attempts to change the player's profile and a transaction or transactions that appear to be linked amount to 4000 NAF or more. When a transaction or a series of transactions that appear to be linked amounts to more than 4000 NAF (or equivalent in another currency), the CDD measures are applied automatically (the wagering of a stake, the deposit of funds or the collection of the winnings through the withdrawal of the funds constitute a transaction in such cases). Periodic reviews of the existing records and ongoing monitoring of the transactional patterns of the regular players also form an integral part of the CDD measures.

As part of combating money laundering, fraud and terrorist financing, players' IP addresses are tracked via an embedded tool in the proprietary antifraud system in order to ensure the site is accessed from nonrestricted countries. This measure also helps detect suspicious activity such as attempts to set up multiple accounts by the same individual, or block individuals who have been blacklisted or self excluded. The proprietary software also monitors data as regards the players' transaction history, betting amount, information on wins and losses, players' geolocation, pattern of gambling activity and duration of playing. These tools may be used in instances where a client risk's rating is deemed to be high due to presence of some behavioral or transactional triggers that point to a potential AML/CFT breach.

In cases where the CDD measures cannot be applied, the account gets locked during an attempt to complete CDD and ultimately the business relationship with the client gets terminated due to the failure to satisfy AML/ CFT legislative requirements and the funds are refunded back to the client through the same payment channel and account used to deposit the funds.

## **Customer Acceptance Policy (CAP)**

Aspro N.V. implements a formal **Customer Acceptance Policy (CAP)** to establish clear guidelines for the acceptance, onboarding, and continued engagement of customers, in alignment with its risk-based approach to Anti-Money Laundering (AML), Counter Terrorism Financing (CTF), and Counter Proliferation Financing (CPF) compliance obligations.

This policy defines **which customer types are acceptable**, **under what conditions** they may be onboarded, and **when service must be refused or terminated**.

### **Principles of Customer Acceptance**

The acceptance of a customer must be based on:

- A clear understanding of the customer's identity, source of funds, and transactional behavior.
- Risk scoring and profile categorization (low, medium, high).
- Completion of required Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) based on risk level.
- Screening against sanctions, PEP, watchlists, and adverse media.

The Company reserves the right to reject or terminate any customer relationship that presents excessive risk or fails to meet verification standards.

### **Categories of Customers Not Accepted**

Aspro N.V. does **not establish or maintain** business relationships with the following categories:

- Individuals providing false, forged, or unverifiable documentation.
- Persons under the age of 18 or otherwise considered minors.
- Individuals from jurisdictions subject to sanctions, embargoes, or identified by FATF as high risk or noncooperative.
- Politically Exposed Persons (PEPs), or their close associates/family, who are assessed to pose a high residual risk after EDD.
- Customers with known links to criminal activity, terrorism, or proliferation financing.
- Customers who refuse to complete KYC/CDD processes or are uncooperative.
- Persons using third party payment methods not registered in their own name.
- Anonymous users or users attempting to bypass geo-blocking or IP detection systems.

### **Onboarding Thresholds and Risk Tiers**

Customers are accepted based on a **tiered risk model**:

- **Tier 1 (Low Risk):** EEA residents with a single funding source and standard wagering behavior.
- **Tier 2 (Medium Risk):** Users with moderate transaction volume or from regions with partial AML risks.

- **Tier 3 (High Risk):** PEPs, offshore clients, cryptocurrency users, or customers with complex ownership structures. Require EDD and managerial approval.
- **Tier 4 (Unacceptable Risk):** Customers that fall under banned categories listed above.

The Compliance Team reviews all high risk applications before activation.

### **Review and Approval**

- All high risk customer onboarding requires **preapproval by the Compliance Officer or designated senior personnel**.
- The CAP is reviewed at least annually, or upon any regulatory change, and approved by the Board of Directors.

### **Termination Based on Risk Profile**

If a customer's profile changes or exhibits high risk behavior post onboarding (e.g., unusual transactions, fraud indicators), the relationship may be suspended or terminated following internal review. All such cases are documented and, where appropriate, reported to the FIU.

## **Enhanced Due Diligence**

Enhanced Customer Due Diligence and Ongoing Monitoring are applicable to cases that receive a high risk rating. Such examples may include doubts as to the authenticity of the documents, a high risk third country location of the customer, a Politically Exposed Person (PEP) status of a potential customer, unusual behavioral patterns and therefore require additional investigations in the form of additional verification checks, adverse media screening or requests to provide additional documentation as regards the source of wealth, source of funds, utility bills, etc.

Company undertakes a list of Enhanced Due Diligence measures that may include:

- Obtaining additional information on the intended nature and purpose of the business relationship.
- Obtaining information of the source of funds or source of wealth of a customer.
- Obtaining additional information on the intended purpose of a transaction.
- Obtaining, and where appropriate verifying, additional information on the customer and beneficial owner.
- Searching the Internet for corroborating activity information consistent with the customer's transaction profile

- Obtaining, where possible, negative information about the customer and his/her business activities through adverse media searches.
- Increasing the frequency of reviews on a customer.
- Performing a credit search on a customer
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
- Requesting data relating to transaction and trading history
- Request business documents, financial statements, or KYC documents to be certified or notarized by an independent third party (e.g. accountant or solicitor or public notary)
- Request a meeting in person with the customer or a video call to verify the customer's identity
- Corroborating the identity information received from the customer, such as a national identity number, with information in third party databases or other reliable sources.
- Tracing the customer's IP address
- All high risk customers are reviewed by the Compliance team prior to onboarding.

## **PEPs (Politically Exposed Persons)**

A Politically Exposed Person (PEP) is defined by the FIU s 'Individuals entrusted with prominent public functions. The definition of a 'prominent public function' will vary according to the nature of the function held by a person. The Firm is required to understand the nature of each position held and whether the function gives rise to the risk of largescale abuse of position.

The Politically Exposed Persons (PEPs) applications are handled by the senior management team whose approval is necessary to transact with such individuals and an internal register of such cases is kept by the Compliance officer office.

A PEP is an individual who recently held ( in the last 12 months) or is currently holding a prominent public position such as a head of state, member of the Parliament, government, directors of international organizations etc.

Family members of PEPs and close associates are also considered PEPs, so their applications are also treated as high risk by the Antifraud team and relevant risk management procedures are activated when processing such requests through the senior management.

If the Compliance Team identifies a PEP as a beneficial owner of a merchant entity, the Company will not automatically treat the legal entity as a PEP only because a PEP is a beneficial owner. However, the Compliance Team will apply a risk-based approach to the entity to assess the risk posed by the involvement of that PEP and, after making this risk assessment, the Company will apply appropriate measures in accordance with this procedure. These could range from applying Standard Due Diligence measures in cases where the PEP is just a figurehead for an organization (this will vary according to the circumstances of each entity but could be the case even if PEP sits on the board, including as a nonexecutive director). However, if it becomes apparent the PEP has significant control or the ability to use their own funds in relation to the entity, the Firm will apply Enhanced Due Diligence measures.

### **PEP Risk Factors and Assessment**

PEPs may pose various levels of Money Laundering and Terrorist Financing risk dependent on strength of certain risk factors. The Company also considers a PEP, family member, or close associate.

The Compliance Team is required to manually handle this process and not rely on third party service providers. The Team is required to diligently assess these risk factors for each identified PEP or known close associate or family member of a PEP.

After doing so, they must determine if the PEP represents a high risk or a low risk, escalate it to Higher Manager for the final decision and this decision must be recorded in the customers' file.

### **Identification of PEP and Mitigation Measures**

Compliance Team required to undertake certain measures when they identify and verify a proposed customer PEP, or family member, or known close associate of a PEP's status.

Upon verification of the PEP, or family member or known close associate of a PEP's status. The following measures should be applied:

- Obtain signoff, as a minimum, from Higher Management before proceeding with the relationship.
- Take “adequate measures” to establish the customer’s source of wealth and source of funds relevant to the proposed business relationship or transaction.
- Conducted enhanced ongoing monitoring of the business relationship.
- Review PEPs on an annual basis to ensure information is still accurate and up to date PEP due diligence measures

If the Firm determines that a PEP represents an elevated risk of Money Laundering and Terrorist Financing, Compliance Team conducts EDD measures on them. EDD measures that the Company’s employees may apply to high risk PEPs include:

- Immediate escalation to the Higher Management for review, the decision whether the business relationship should be established.
- If Higher Management will determine if the risks posed by a PEP are higher than the Company can effectively mitigate, the Company will not enter into or continue a business relationship with a PEP.
- Examine whether the Company knows a PEP face-to-face.
- Intrusive steps to establish the source of wealth and funds
- Examine nature of the proposed business relationship with a PEP.
- The potential for the Company’s products and services to be misused for the purposes of corruption.
- Undertake frequent and thorough monitoring of the relationship to ascertain whether it should be maintained.
- Reference public domain information such as websites of parliaments and governments, reliable news sources, and work by reputable pressure groups focused on corruption risks such as Transparency International or Global Witness to understand the nature of position PEP holds

If the Firm determines that a PEP represents an elevated risk of Money Laundering and Terrorist Financing, Compliance Team conducts EDD measures on them. EDD measures that the Company’s employees may apply to high risk PEPs include:

## **Ongoing Monitoring**

The Firm conducts ongoing monitoring on two levels:

1. Account monitoring
2. Transaction monitoring

The Company conducts manual review of fiat activities and a retrospective analysis of customer behavior. It considers previous checks and data related to the customer. It allocates a specific risk rate, and all high risk customers are regularly reviewed.

Risk score is assigned to each transaction, based on the following information:

- Higher than average Transaction Value:

The total historical transactional average of a customer will be assessed. Where a transaction exceeds the customer's typical behaviors, these transactions will receive additional weighting.

Activities in a customer's account are being monitored as well analyzing Deposit/withdrawals trends. The Company subjects all accounts for review on a regular basis to determine if account activities are in keeping with the customer's standard and ongoing profile.

When conducting deposit monitoring Company analyze the following:

- The customer profile and risk score history
- Due diligence documents
- The customer incoming funds history
- All transactions made by the customer since the beginning of the relationship such as deposits, betting, losses and winnings
- Number of accounts held by the customer and their transaction history

Aspro N.V is obliged to conduct ongoing monitoring of business relationships with their clients. Compliance Team conducts ongoing monitoring of clients in the following ways in accordance with the Company's risk-based approach:

Screening of clients against PEP, Sanctions, and Adverse Media on a regular basis. Any alerts considered to be true matches may trigger an Event Driven Review.

i. Event Driven Reviews

Certain events will trigger an Event Driven Review which may, depending on the type of changes flagged, require a full customer due to diligence refresh.

Aspro N.V, through the course of its daily activities, obtains the information that brings a question to the accuracy of the customer due diligence information collected, or if suspicion arises, then the customer will undergo an immediate review, irrespective of their risk status.

ii. Periodic Reviews

Aspro N.V. has an obligation to ensure that customer due diligence information is relevant and kept up to date via regular client reviews. The extent to which clients' reviews are undertaken will be determined by using a risk based approach and applied in accordance with the risk rating applied to the customer during the customer risk assessment. The Company has a customer review process based on the High, Medium, and Low risk factors assigned to its customers

The periodic reviews are conducted in line with the client's risk score and profiles are as follows.

High Risk – Every year. This will entail establishing the following:

- Reconfirmation of Address
- Reconfirmation of Source of Funds and Wealth
- Screening for adverse news
- Complete review of transaction profile, including new products requested

Medium Risk – Every two years. This will entail establishing the following:

- Reconfirmation of Address
- Reconfirmation of Source of Funds and Wealth
- Screening for adverse media
- Complete review of transaction profile, including new products requested

The information obtained during the review will be assessed to determine if the medium risk rating still applies.

Low Risk – Every three years. However, reviews will be undertaken when trigger events occur such as:

- where the firm had come into possession of news or information that brings doubt to the accuracy of the current CDD information held
- when the Firm has identified activity deemed to be suspicious
- This review will entail establishing the following:
  - Reconfirmation of Address
  - Screening for adverse media
- The information obtained during the renewal will be assessed to determine if the low risk rating still applies.

The company's procedures are reassessed whenever the National Risk Assessment (NRA) is updated, ensuring that internal controls, risk ratings, and related measures remain aligned with current national risk priorities and regulatory expectations. Confirm procedures are reassessed whenever the NRA is updated

## **Ongoing PEP Screening**

Aspro N.V. conducts continuous, automated screening of all customers against updated Politically Exposed Person (PEP) lists for the entire duration of the business relationship. PEP status may change at any time due to elections, public appointments, or new information disclosed in reputable sources; therefore, initial PEP checks performed at onboarding are not sufficient on their own. The Company's screening system refreshes PEP data daily and immediately triggers alerts when a customer, beneficial owner, or associated individual is newly identified as a PEP or becomes linked to a PEP through family or close associations. Any positive match is promptly escalated to the Compliance Officer for review. In such cases, Enhanced Due Diligence (EDD) measures are applied, including verification of source of wealth, source of funds, ongoing transactional scrutiny, and senior management approval. Where a PEP presents a disproportionate risk that cannot be effectively mitigated, the Company may restrict or terminate the business relationship.

### **Termination of Business Relationships**

Aspro N.V. upholds a strict and transparent procedure for terminating customer relationships that pose an elevated risk of financial crime or fail to meet Customer Due Diligence (CDD) obligations. These measures ensure ongoing compliance with applicable AML, CTF, and CPF regulations while protecting the integrity of the platform.

#### **Grounds for Termination**

The company may terminate a customer relationship under the following conditions:

The individual is found to be engaging in activity suggestive of money laundering (ML), terrorist financing (TF), or other suspicious financial behavior.

The customer fails to provide the required CDD documentation or refuses to cooperate with verification procedures within a specified timeframe.

The individual is assessed as posing a high ML/TF risk based on updated risk profiling, behavioral indicators, or jurisdictional exposure.

#### **Termination Procedure**

Aspro N.V. follows a controlled and documented process when discontinuing a business relationship:

Senior management reviews and formally approves all termination decisions.

A final risk-based review of the customer's account activity is conducted prior to closure.

If the review identifies unusual or potentially illicit transactions, a Suspicious Transaction Report (STR) is filed with the Financial Intelligence Unit (FIU).

All customer records, including identification details and transactional history, are securely retained for at least five years in accordance with legal and regulatory requirements.

### **Third party Reliance for Customer Due Diligence**

Aspro N.V may utilize third party service providers to perform specific components of its Customer Due Diligence (CDD) obligations. However, such reliance is governed by a strict regulatory framework to ensure that all processes remain fully aligned with Anti-Money Laundering (AML), Counter Terrorism Financing (CTF), and Counter Proliferation Financing (CPF) requirements. Regardless of any delegation, the company retains full accountability for the proper execution of CDD measures and overall compliance outcomes.

### **Oversight and Accountability**

To ensure transparency and regulatory integrity in third party collaborations, Aspro N.V enforces the following controls:

- Formal written agreements are established with all CDD service providers, clearly defining their duties, compliance standards, and data sharing obligations.
- The company guarantees immediate access to all customer identification records collected by third parties when required.
- Periodic audits and performance reviews are conducted to verify adherence to AML/CTF/CPF protocols.
- Despite any delegation, Aspro N.V independently determines key compliance factors, such as:

The customer's Politically Exposed Person (PEP) status

Ongoing risk classification and updates

Transaction monitoring and red flag detection

### **Conditions for Acceptable Third party Reliance**

To qualify for CDD reliance, the third party entity must meet specific regulatory standards:

- Must be a regulated institution, supervised under a recognized AML/CFT/CPF legal regime.
- Must maintain an independent business relationship with the customer (i.e., not acting solely as an intermediary for Aspro N.V).
- Must operate in a jurisdiction with equivalent AML/CTF/CPF standards, subject to favorable evaluation through the company's jurisdictional risk assessment process.

Aspro N.V evaluates third party jurisdictions using internationally recognized intelligence sources, such as FATF mutual evaluations and global AML risk indices, to ensure that outsourcing does not introduce compliance vulnerabilities.

### **Outsourcing vs. Third party Reliance: Key Distinction**

Aspro N.V recognizes the difference between outsourcing and third party reliance:

- In third party reliance, the external party conducts specific CDD tasks independently, but the regulatory liability remains with Aspro N.V
- In outsourcing arrangements, the third party acts under the company's direct instructions, adhering strictly to internal procedures and controls.

Regardless of the structure, Aspro N.V maintains full oversight and control over customer risk assessments, onboarding decisions, and relationship management.

## **Sanction Management, FATF Blacklist, License Restrictions**

Aspro N.V. operates under the Curacao online gaming license and is therefore banned from offering its online services in Aruba, Bonaire, Curacao, France, the Netherlands, Saba, Statia, St. Maarten, Singapore and the USA. It does not operate in countries where there is a total ban on gambling such as China, Turkey, Brunei, Cambodia, Japan, Qatar, Lebanon, Poland inter alia or where the Company is required to obtain a local gambling license in order to operate locally ( USA, UK, EU countries for instance).

In light of the fact that the Curacao belongs to the Dutch Caribbean, under article 1(1) of the Kingdom Sanctions Law (Rijkssanctiewet) provisions of binding EU legal acts are effective from the date of their entry into force in Curaçao in the same way as in the Member States of the European Union. Consequently, the Regulations are also directly implemented in Curacao.

The Company, being a Curacao based entity which transacts with the EU and the EU based payment partners, complies with the following regional sanctions lists:

European Union Sanctions List: [EU Sanctions Website](#)

UK Sanctions List (OFSI): [UK Sanctions Search](#)

UK Consolidated Sanctions List: [Gov.uk Sanctions Collection](#)

United Nations Security Council Consolidated List: [UN Consolidated List](#)

U.S. State Department List of Foreign Terrorist Organizations: [State.gov FTO List](#)

U.S. Department of Treasury OFAC SDN List: [OFAC Sanctions Search](#)

The Company's primary goal in this regard is to prevent making payments to designated persons and sanctioned entities and/or serve customers from FATF blacklisted countries such as Democratic People's Republic of Korea, Iran, Sudan and countries that are on the State Sponsors of Terrorism list by the U.S. Department of State i.e. Cuba, North Korea, Iran and Syria (<https://www.state.gov/statesponsorsofterrorism/>). In unlikely circumstances where a payee or a customer are identified as a designated person, payments will not be processed and an internal SAR/STR report will be submitted to the Compliance officer office for further regulatory processing if necessary.

Aspro N.V. ensures that all customers, counterparties, and transactions are screened against updated sanctions lists on an ongoing basis, using automated screening tools. Upon identification of a potential or confirmed match, the account is immediately frozen, and all transactions are halted pending internal investigation and potential reporting to the Financial Intelligence Unit (FIU).

The Compliance Officer is responsible for reviewing all sanctions alerts. Confirmed designations result in asset blocking and the filing of a Suspicious Transaction Report (STR).

Third party payment processors and affiliated service providers are contractually required to conduct sanctions screening and block transactions involving designated individuals or jurisdictions.

Sanctions procedures are tested quarterly, and screening databases are updated daily to ensure full regulatory compliance.

## **Record Keeping**

The Company is maintaining all necessary records related to transactions (both domestic and international) for a minimum of five years to ensure compliance with information requests from competent authorities. All records are detailed enough to allow for the reconstruction of individual transactions (including amounts and types of currency involved, if applicable), to provide, when necessary, evidence for the prosecution of criminal activity. Additionally, all records obtained through Customer Due Diligence (CDD) measures, such as copies or records of official identification documents (e.g., passports, identity cards, driving licenses, or similar), account files, and business correspondence, are retained for at least five years following the termination of the business relationship or the date of an occasional transaction. CDD information and transaction records are readily accessible to domestic competent authorities upon proper legal request.

The company adheres to rigorous recordkeeping practices to ensure compliance with AML/CTF/CPF regulations. We prioritize maintaining secure, accurate, and accessible documentation to support regulatory compliance, internal audits, and the integrity of the gaming industry.

To meet legal requirements, the company retains key documentation for a minimum of five years. These records include all customer identification details collected during the onboarding process, transaction data, suspicious activity reports (SARs) submitted to the Financial Intelligence Unit (FIU), training records for employees, and audit logs. These documents are critical for demonstrating compliance with the company's AML/CTF/CPF procedures and for assisting in any potential regulatory review or investigation.

## **Suspicious Activity Reporting**

In cases where employees of the Company know, suspect, or have reasonable grounds to believe that a person is attempting to finance terrorism or launder money, a relevant reporting protocol is activated, and a suspicion report must be submitted to the nominated officer who then determines whether there are grounds for further regulatory action. Unusual gambling patterns are investigated first to determine whether the exact nature of the transaction is just unusual or there are grounds to believe that it may be affiliated with the proceeds of a crime. According to article 1 of the Norut (National Ordinance on the Reporting of Unusual Transactions) it is an internet gambling entity's duty to report unusual transactions (A transaction that is considered as such on the basis of certain indicators, pursuant to Article 10 of the NORUT.) through the FIU Curacao's goAML portal which has been in use since January 1, 2021. Therefore, if the nominated officer determines that the internally reported suspicious activity should be disclosed to the regulatory authorities, he does so via the portal to comply with the Company's AML/CFT/CPF reporting obligations and then determines whether the business relationship with the suspected customer should be paused or terminated.

Aspro N.V maintains a proactive and structured approach to identifying and reporting suspicious activity that may indicate money laundering (ML), terrorist financing (TF), or proliferation financing (PF). This includes behavioral anomalies, significant or unexplained financial movements, and any interaction involving jurisdictions or individuals known to present elevated risk.

All employees are required to remain vigilant and immediately escalate any concerns to the appointed Compliance Officer. Once notified, the Compliance Officer performs a detailed assessment to determine whether further internal action or an external report to the appropriate authority is necessary.

### **Identifying Unusual Transactions**

Transactions are considered unusual if they significantly deviate from a customer's typical financial behavior or profile. Common red flags include:

- Large, unexpected transactions that are inconsistent with known income or gambling activity
- Transfers involving unidentified third parties or high risk jurisdictions
- Financial operations that lack a lawful or logical purpose

Monitoring tools are used to flag these transactions automatically, with each flagged case escalated to the Compliance Officer for deeper investigation.

### **Categories of Transactions Warranting Review**

In accordance with Curaçao's AML/CTF regulatory framework, Aspro N.V treats the following types of transactions as unusual and subject to further scrutiny:

- Previously reported transactions: Any transaction already submitted to law enforcement or regulatory bodies due to ML/TF suspicion is immediately categorized as unusual.
- Transactions with sanctioned individuals or entities: Dealings involving any party listed under the Sanctions National Ordinance (N.G. 2014 no. 55) are automatically escalated for further review.
- Transactions at or above NAF 5,000: This applies regardless of payment method whether via cash, check, electronic transfer, or other digital means. Examples include:
  - Deposits or withdrawals meeting or exceeding the threshold
  - Purchases of gaming tokens, credits, or chips above NAF 5,000
  - Payouts or redemptions reaching this benchmark

Note: Transactions may be considered collectively if they form part of a linked pattern or series that meets or exceeds the NAF 5,000 threshold in a single gaming day.

### **Presumptive Suspicion and Escalation**

If a transaction shows signs indicative of money laundering or terrorist financing even without conclusive proof it must be treated as suspicious and documented accordingly. The Compliance Officer then evaluates whether it meets the criteria for submission to the Financial Intelligence Unit (FIU).

### **Maintaining Confidentiality**

To safeguard the integrity of the investigation and comply with legal standards, Aspro N.V enforces strict confidentiality in all matters related to suspicious activity reporting (SAR). Employees are explicitly prohibited from:

- Disclosing SARrelated information to the customer(s) involved
- Discussing the matter with unauthorized colleagues or external parties

Access to SAR documentation and discussions is restricted solely to the Compliance Officer and designated compliance personnel. All employees receive training to reinforce the importance of confidentiality, particularly regarding the risks of “tipping off” and the consequences of noncompliance.

Violations of this policy are treated as serious disciplinary offenses and may lead to termination of employment or other corrective measures.

By cultivating a culture of alertness and discretion, Aspro N.V reinforces its commitment to regulatory compliance, protects the integrity of its operations, and plays an active role in detecting and disrupting financial crime.

## **Unusual Transactions**

An unusual transaction is identified as any transaction that deviates from the expected behavior based on the player’s profile. The foundational step in recognizing such transactions is to ensure sufficient knowledge about the player. In compliance with the NORUT legislation, the company has established objective and subjective indicators to assess whether a customer’s transaction should be classified as unusual. Management is responsible for ensuring that all staff members receive specific training and clear guidance on recognizing and properly documenting such transactions. All unusual transactions must be reported to the compliance officer.

To report unusual transactions to the Financial Intelligence Unit (FIU) of Curaçao Company must through the goAML portal

[https://portal.fiucuracao.cw/goAMLWeb\\_PRD/Home](https://portal.fiucuracao.cw/goAMLWeb_PRD/Home) prior obtaining credentials from FIU. After a report is submitted, a confirmation of receipt will be issued by FIU Curaçao.

suspicious activity may include using an intermediary for document related requests; source of wealth does not match the reported financial data; frequent changes of ownership in a short time; lack of willingness to provide due diligence documentation.

## **Employee Training**

The Company requires all relevant employees to complete AML/CFT/CPF training covering their area of responsibility at least annually. The focus of the training programs is to make sure that the employees follow the right protocols to verify customer information and can identify suspicious activity both internally and externally. The employees are made aware regularly of their legal obligations to report suspected breaches to their senior manager and who then contacts the Compliance officer office to discuss the internally submitted SAR/STR report as any acts of collusion, manipulating records or bypassing KYC protocols will result in committing a criminal offense for which they will be tried if caught.

The doctrine "willful blindness" is a recurring theme of the internal training programs due to its massive legal implications for the employees who may have deliberately avoided "the knowledge of the facts" and therefore exposed themselves to being criminally liable for the ML/FT offenses. Furthermore, The Company implements the Know Your Employee (KYE) policy which centers around initiatives which help acquire a better knowledge of the employees' character and behavioral patterns after they successfully passed a background check to be able to detect conflicts of interests or suspicious activity occurring in the workplace.

All personnel, whose duties include the handling of Clients' business, are to be adequately trained with respect to the procedures and the provisions of the Prevention of Money Laundering Act.

The level of training provided to individuals is to be appropriate to their role and seniority within the Company. In any case all Employees must have the proper training on ML/TF prevention prior to the commencement of their duties at the Company which involve the ML/TF risk.

Compliance officer prepares and implements, on an annual basis (or whenever deemed necessary), an educational training program (training plan) for staff depending on the needs of the Company regarding the prevention of using the financial system for money laundering or other illicit purpose, including preventive developments and practical methods and trends used.

Employees in the betting and gambling industries are on the front lines of AML compliance. Aspro N.V. conducts its operations with a high standard of ethics, ensuring full compliance with laws and regulations governing financial transactions. The company has implemented policies and procedures for screening employees for criminal records, as part of its ongoing commitment to integrity.

To ensure the integrity and competence of personnel engaged in activities relevant to Anti-Money laundering (AML) and counterterrorist financing (CTF) obligations, the Company maintains a structured Employee Screening Program in accordance with CGA AML Regulation V.4. Please see **Appendix II**.

Aspro N.V.'s employees play a crucial role in Anti-Money Laundering (AML) compliance within the betting and gambling industries. Their actions and vigilance are essential in preventing these sectors from being exploited for money laundering and other illicit activities. They are made aware of the fact that failing to report potential breaches of AML Policies may lead to administrative and criminal charges.

The Company's employees, especially those in client facing roles or positions that involve handling financial transactions, must have a thorough understanding of the company's AML policies and procedures. This includes knowing the types of transactions that should be considered suspicious, the process for reporting such transactions, and the importance of maintaining client confidentiality.

A key part of an employee's role in AML compliance is to be vigilant and identify any activities that seem unusual or do not fit with the normal behaviour of a client. This could include large and inconsistent bets, frequent changes in betting patterns, or transactions that seem to have no apparent purpose other than to move money through the system.

Once an employee identifies a potentially suspicious transaction, they must report it through the appropriate channels to the Compliance Officer. The reporting protocol involves filling out a Suspicious Activity Report (SAR) and using the company's internal reporting system. Employees are trained on how to report suspicions and the importance of doing so promptly on an annual basis or more frequently in line with the needs of a particular department.

Employees involved in client onboarding or account management are responsible for conducting due diligence checks on clients. This includes verifying their identity, understanding the source of their funds, and ensuring that they are not listed on any sanctions or watch lists. Employees are trained on how to conduct such checks diligently and escalate any concerns where necessary.

Employees involved in AML compliance at Aspro N.V. understand the importance of maintaining the confidentiality of their reports and any information related to suspicious activities. They are made aware of data protection laws and ensure that client information is handled in compliance with these regulations.

Aspro N.V. upholds the highest standards of integrity and professionalism among its personnel, recognizing employees as critical to the company's Anti-Money Laundering (AML), Counter Terrorism Financing (CTF), and Counter Proliferation Financing (CPF) compliance framework. In line with Regulation V.4 of the CGA AML Guidelines, the company maintains a formal Employee Screening Program, applied both prior to employment and on an ongoing basis thereafter.

#### 1. Pre-employment Screening

Before onboarding any new employee, especially those in sensitive, client facing, or compliance related roles, the company conducts thorough background checks, including:

- Verification of identity and right to work using government issued documentation.
- Criminal background checks to detect any prior financial or integrity related offenses.
- Employment and reference verification to confirm qualifications and experience.
- Sanctions and PEP screening, using independent screening tools and global watchlists.

Candidates failing to meet the company's integrity or risk criteria are not employed.

## 2. Ongoing Employee Screening

Aspro N.V. continues to assess employee suitability after hiring through:

- Annual rescreening of employees in AML/CTF sensitive roles.
- Event driven screening, such as when suspicious activity, misconduct, or role changes occur.
- Monitoring for changes in sanctions exposure, PEP status, or relevant legal/regulatory risks.

All employee screening records are retained securely and confidentially, in compliance with data protection laws, for a minimum of five (5) years.

## 3. Training and Awareness

Employees, particularly those involved in onboarding, account management, or transaction processing, receive annual AML/CTF training tailored to their roles. This training ensures staff understand:

- The company's AML/CTF/CPF obligations.
- How to identify unusual behavior, such as:
  - Large or inconsistent bets.
  - Suspicious patterns of deposits/withdrawals.
  - Anonymous or third party payments.
- How and when to file a Suspicious Activity Report (SAR).
- The importance of confidentiality and client data protection.

Employees are made aware that failure to comply with AML/CTF obligations may lead to disciplinary, administrative, or criminal consequences.

Compliance officer shall evaluate the adequacy of the seminars, and the training provided to the staff and maintains detailed data regarding the seminars/ programs carried out, such as:

- contents of the training
- the date, title and duration of the seminar and the names of the trainers,

- names of employees participating in the seminar/training by branch/department and by position (management staff, officers, newcomers etc.),
- the persons who were unable to attend the training accompanied with the reason for non attendance
- whether the lecture/seminar was organized internally or offered by an external agency or consultants.
- An ongoing training plan.

## **Audit Function**

To comply with Curaçao's updated gaming regulations, Company performs an independent audit focusing on Anti-Money Laundering (AML), Counter Terrorism Financing (CTF), and Counter Proliferation Financing (CPF) procedures and appoints an independent auditor, either external or an internal team with AML expertise, who must be approved by the Gaming Control Board to prevent conflicts of interest. The audit follows both international standards and specific requirements from the Gaming Control Board, examining policies, risk management effectiveness, transaction monitoring systems, staff training adequacy, reporting mechanisms, and compliance with KYC (Know Your Customer), KYB (Know Your Business), and Customer Due Diligence (CDD) protocols.

After completion, the auditor submits a report detailing findings and recommendations to Company's senior management and the Gaming Control Board, with the company committed to implementing any necessary corrective actions. The Gaming Control Board maintains oversight of the audit process and can request additional documentation or perform inspections as needed to verify compliance. The Company acknowledges that noncompliance identified through audits or Board evaluations could lead to penalties, including fines, operational restrictions, or even suspension or revocation of its gaming license, underscoring its commitment to full cooperation with the Gaming Control Board in implementing corrective actions and maintaining compliance.

### **Audit Process and Evaluation**

The audit process follows both international standards and specific requirements set by the Gaming Control Board. Key steps include:

1. Evaluation of Policies and Procedures: Ensuring that the company's AML/CTF/CPF policies are updated and fully compliant with current legal requirements.
2. Risk Management Assessment: Reviewing how risks are identified and mitigated, and ensuring effective risk management strategies are in place.
3. Transaction Monitoring Review: Assessing the effectiveness of systems used to detect suspicious transactions and ensuring proper reporting.
4. Staff Training Evaluation: Verifying that training programs meet regulatory standards and that employees are properly equipped to detect and report suspicious activities.
5. Reporting Mechanism Audit: Checking how suspicious transactions and compliance issues are reported, ensuring that all processes are streamlined and accurate.

6. Customer File Review: Auditing the KYC, KYB, and CDD protocols to ensure that customer identification and risk assessment procedures are followed.

### **Audit Report and Findings**

After the audit, the independent auditor provides a detailed report to the company's senior management and the Gaming Control Board. This report outlines the findings, recommendations, and any issues identified during the audit. Aspro N.V. will act on the auditor's recommendations, implementing corrective actions within an established timeframe.

### **Gaming Control Board's Role**

The Gaming Control Board, which oversees AML/CTF/CPF compliance for all licensed operators, reviews the audit results to ensure that the company is in full compliance. The Board may:

- Review the Audit Report: Analyzing the auditor's findings to assess compliance and highlight any concerns.
- Conduct Onsite Inspections: Verifying audit findings through visits to the company's premises to evaluate the effectiveness of corrective actions.
- Perform Interviews and Documentation Analysis: Interviewing relevant staff and reviewing supporting documents to better understand the company's AML/CTF/CPF practices.

Aspro N.V. maintains an audit trail and full documentation of all internal audit activities for a minimum of five (5) years and makes such records immediately available to the Curaçao Gaming Control Board (GCB) upon request. The Company is committed to transparency, accountability, and continuous improvement in its AML/CTF/CPF compliance framework.

### **Regulatory Access and Cooperation**

Aspro N.V. fully acknowledges the supervisory and enforcement authority of the Curaçao Gaming Control Board (GCB) and commits to complete, proactive cooperation with all regulatory examinations and oversight activities. To this end, the company grants the GCB and any other legally empowered authority unrestricted, immediate, and comprehensive access to all data, systems, records, and personnel necessary for the assessment of its Anti-Money Laundering, Counterterrorism Financing, and Counter Proliferation Financing (AML/CTF/CPF) framework.

This includes, but is not limited to:

- Customer due diligence records
- Transaction histories and monitoring data

- Internal risk assessments
- Policies and procedures
- Communication logs and training materials
- Audit trails, reports, and logs
- Compliance related systems and platform

Access shall be granted for both onsite and remote inspections, including the right to request supplementary documentation, system walkthroughs, and clarifications. Aspro N.V. ensures that all required information is readily retrievable, promptly provided upon request, and securely maintained for a minimum of five (5) years, or longer where legally mandated. Furthermore, the company commits to full cooperation with any post inspection findings, including corrective action plans and remedial steps as directed by the GCB.

# Appendix I Score Calculation

HOW TO USE THIS?  
1. Only yellow and blue fields have to be filled.  
2. Comment section is available, however, it is not necessary for calculation of risk level.  
3. Majority of questions has dropdown list or checkbox. Correct answer(-s) should be selected.

|                        |      |
|------------------------|------|
| NEW total score:       | 0.00 |
| NEW risk level:        | Low  |
| Onboarding specialist: |      |
| Last update date:      |      |

| Category     | Score       |
|--------------|-------------|
| low          | 0-2.5       |
| medium       | 2.5-3.2     |
| high         | 3.2 or more |
| unacceptable |             |

|             |  |
|-------------|--|
| Client no.: |  |
| Name:       |  |

| Risk Category                                 | Question                                                                                            | Risk score | Risk level | Additional comments |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------|------------|------------|---------------------|
| Client                                        | Customer's Age                                                                                      |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
| Geography                                     | Customer's Citizenship                                                                              |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
| Geography                                     | Customer's Second Citizenship                                                                       |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
| Geography                                     | Customer's Country of Birth                                                                         |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
| Geography                                     | Customer's Country of Residence                                                                     |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
| Client                                        | Does Customer have the status of PEP/RCA (Politically Exposed Person/Relative and Close Associate)? |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
| ACCOUNT PROFILE                               |                                                                                                     |            |            |                     |
| Client                                        | Purpose of account registration?                                                                    |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
| FUND SOURCE AND INCOME STATUS                 |                                                                                                     |            |            |                     |
| Client                                        | Source of funds                                                                                     | average    |            |                     |
|                                               |                                                                                                     |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
| Client                                        | Source of wealth                                                                                    | average    |            |                     |
|                                               |                                                                                                     |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
| INTENDED ACCOUNT ACTIVITY (DEPOSITS)          |                                                                                                     |            |            |                     |
| Transactions                                  | Average frequency of transactions                                                                   |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
| Transactions                                  | Expected total value of transactions per period (NAP)                                               |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
| Transactions                                  | Types of incoming payments                                                                          | average    |            |                     |
|                                               |                                                                                                     |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
| INTENDED ACCOUNT ACTIVITY (OUTGOING PAYMENTS) |                                                                                                     |            |            |                     |
| Transactions                                  | Average frequency of transactions                                                                   |            |            |                     |
|                                               |                                                                                                     |            |            |                     |
| Transactions                                  | Expected total value of transactions per period (NAP)                                               |            |            |                     |
|                                               |                                                                                                     |            |            |                     |

| Risk Category:        | To be: | Sum: | Weight: |
|-----------------------|--------|------|---------|
| Client                | 20%    | 0    |         |
| Geography             | 20%    | 0    |         |
| Products and Services | 20%    | 0    |         |
| Transactions          | 20%    | 0    |         |
| Channels              | 15%    | 0    |         |
| Other                 | 5%     | 0    |         |
|                       |        | 0    |         |

|                         |                                                                    |         |  |                                                                        |
|-------------------------|--------------------------------------------------------------------|---------|--|------------------------------------------------------------------------|
| Transactions            | Types of outgoing payments                                         | average |  |                                                                        |
| Transactions            |                                                                    |         |  |                                                                        |
| Transactions            |                                                                    |         |  |                                                                        |
| Transactions            |                                                                    |         |  |                                                                        |
| Transactions            |                                                                    |         |  |                                                                        |
| Transactions            |                                                                    |         |  |                                                                        |
| Transactions            | Reasons for outgoing payments                                      | average |  |                                                                        |
| Transactions            |                                                                    |         |  |                                                                        |
| Transactions            |                                                                    |         |  |                                                                        |
| Transactions            |                                                                    |         |  |                                                                        |
| GAMING BEHAVIOUR        |                                                                    |         |  |                                                                        |
| Products and Services   | Please indicate services of interest                               | average |  |                                                                        |
| Products and Services   |                                                                    |         |  |                                                                        |
| Products and Services   |                                                                    |         |  |                                                                        |
| Products and Services   |                                                                    |         |  |                                                                        |
| Products and Services   |                                                                    |         |  |                                                                        |
| CONFIRMATIONS           |                                                                    |         |  |                                                                        |
| Payment Channels        | Channels                                                           | average |  |                                                                        |
| Third-party Involvement |                                                                    |         |  |                                                                        |
| Access                  |                                                                    |         |  |                                                                        |
| Onboarding              |                                                                    |         |  |                                                                        |
| Client                  | Adverse media level                                                |         |  |                                                                        |
| Other                   | Manual risk level adjustment based on the expert judgement (±0.5): |         |  | Comment regarding manual risk adjustment:<br>Summary of the applicant: |

## Appendix II Employee Screening Program

The Employee Screening Program (“Program”) outlines the mandatory standards, controls, and procedures governing the vetting, assessment, and continuous monitoring of all individuals employed or engaged by Aspro N.V.

This Program is implemented to ensure full compliance with CGA AML Regulation V.4, which mandates robust screening procedures both prior to employment and throughout the duration of employment. These requirements support the Company’s commitment to integrity, transparency, and accountability at every level of the organization.

A dedicated Employee Screening Checklist forms an integral component of this Program. Completion of the Checklist is compulsory in every case and must be used to document the Company’s adherence to each screening measure set out herein.

### Scope of the Policy

This Program applies to all individuals who contribute to the operations of Aspro N.V., including:

- Fulltime, parttime, temporary, and contract based employees;
- Senior Management, the Compliance Officer, and all personnel responsible for AML/CTF obligations;
- Individuals performing regulated, sensitive, or risk critical functions through third party or outsourced arrangements.

No individual may commence employment or assume duties in a sensitive or AM related role until all applicable screening activities have been completed and validated.

## **Screening Requirements**

Aspro N.V. must ensure that every individual engaged by the Company is fit, proper, professionally competent, and trustworthy. All screening measures are:

- Risk-based, following the proportionality dictated by each role's sensitivity;
- Consistently applied, following clear, standardized procedures;
- Documented, with all evidence retained to demonstrate regulatory compliance.

The screening framework includes the following components:

1. Pre-employment Screening
2. Fit and Proper Assessment (for designated roles)
3. Ongoing Screening and Monitoring
4. Employee Screening Checklist Completion

## **PreEmployment Screening**

Before any employment offer is finalized, the Human Resources department, working closely with the Compliance Department, must conduct the following checks:

- Criminal Background Check

A formal criminal record check must be obtained to identify any history involving dishonesty, fraud, money laundering, terrorist financing, financial crime, or any conduct inconsistent with the ethical expectations of Aspro N.V.

- Identity Verification

Applicants must provide valid, government issued identification. HR must verify authenticity, accuracy, and consistency with submitted personal information.

- Verification of Academic & Professional Qualifications

All educational, professional, and industry specific qualifications including degrees, certifications, and licenses must be independently validated to ensure legitimacy and relevance.

- Employment History Verification

The Company shall verify prior employment details, including roles, duties, performance, and professional conduct, subject to applicable laws governing reference and information disclosure.

- Professional Reference Checks

At least two professional references must be obtained, reviewed, and recorded. Any unfavourable or inconsistent information must be escalated to the Compliance Department for additional evaluation.

Completion of the Employee Screening Checklist is mandatory before an offer of employment may be authorized.

### **Fit and Proper Assessment**

*Applicable to designated, sensitive, or regulated roles.*

The Fit and Proper Assessment is a structured evaluation that determines whether the individual possesses the integrity, competence, and suitability required to perform functions with regulatory or risk significance.

This assessment considers the following attributes:

- Integrity and Reputation

Assessment of whether the individual demonstrates honesty, ethical conduct, and an absence of adverse regulatory actions, criminal convictions, or reputational risks.

- Competence and Capability

Evaluation of technical knowledge, professional skills, relevant industry experience, and the ability to carry out responsibilities particularly AML/CT related duties.

- Financial Soundness

Where legally permissible, a review of the individual's financial history, such as insolvencies or patterns of financial misconduct, which may indicate elevated risk.

- Independence and Conflicts of Interest

Identification of any real or perceived conflicts that might compromise independence or objectivity. Individuals must demonstrate the ability to act without undue influence or conflicting interests.

The completed Fit and Proper Assessment Form must be reviewed and approved by the Compliance Department and stored alongside the Employee Screening Checklist.

### **Ongoing Screening and Monitoring**

Screening does not end after onboarding. Aspro N.V. maintains continuous oversight to ensure ongoing suitability, integrity, and regulatory compliance.

#### **Periodic Screening**

Employees in sensitive, AML/CTF related, or higher risk positions must undergo **at least annual** reviews, which may include:

- Updated criminal record checks (where legally permitted)
- Reassessments of role suitability
- Performance evaluations focused on conduct and compliance behaviour
- Confirmation of continued independence and conflict free status

#### **Trigger Based Rescreening**

Additional screening is required in response to specific events, including:

- Promotion or transfer to a sensitive or regulated role
- Allegations or evidence of potential misconduct
- Regulatory changes that elevate the risk profile of a role
- External information indicating concerns regarding integrity or suitability

### **Continuous Conduct Monitoring**

Supervisors and the Compliance Department must remain alert to any behaviour, performance issues, or integrity concerns and report them promptly for assessment. For **every** periodic or trigger based rescreening, the Employee Screening Checklist must be updated and retained.

### **Documentation and Record-keeping**

The Company must maintain a complete, well-organized record of all screening activities. This includes:

- Copies of background check reports
- Verification documents and supporting evidence
- Completed Fit and Proper Assessments
- Employee Screening Checklists
- Internal approvals, escalation notes, and decision rationales
- Records of adverse findings and corrective actions taken

All records must be stored securely for a minimum of **five (5) years**, or longer if required by applicable laws or regulations, and must be readily accessible to competent authorities upon request.

### **Responsibilities**

#### **Human Resources**

- Conducts and documents all preemployment screening
- Maintains all personnel screening files
- Ensures thorough completion of the Employee Screening Checklist
- Escalates any concerns to the Compliance Department

#### **Compliance Officer**

- Oversees screening for AML/CTF sensitive roles
- Performs and reviews Fit and Proper Assessments
- Authorizes employment in high risk or regulated positions
- Ensures alignment with CGA Regulation V.4

#### **Senior Management**

- Ensures adequate oversight and resources for screening activities
- Evaluates and approves exceptions or exceptional cases
- Reviews periodic screening and compliance reports

### **Compliance and Enforcement**

Failure to comply with this Program including failure to complete required screening, documentation, or Fit and Proper Assessments may result in disciplinary action, up to and including termination of employment.

Aspro N.V. confirms that this Program fully meets the requirements of CGA AML Regulation V.4. The Program shall be reviewed annually to ensure ongoing regulatory compliance and alignment with best practices.

### **New Employee Screening & Onboarding Checklist**

The following documents and confirmations must be collected and verified before the employee begins their duties.

Copy of national identity card or passport

Work permit, if applicable

Proof of residence

Certificate of clear criminal record

No bankruptcy declaration/letter

Reference letter(s) from previous employer(s)

Professional licenses or certificates relevant to the role

Updated CV (Curriculum Vitae)

Completed Good Repute Questionnaire

Diploma or evidence of higher education

AML and IOM Acknowledgement Letter signed

Privacy Notice signed

Induction & Initial Training Policy / Acknowledgement Form signed

Signed Employment Agreement

## Appendix III Sanctions Policy

### Background

Aspro N.V. is required to comply with a variety of laws and regulations that restrict financial dealings or other interactions with designated individuals, entities, and jurisdictions. This **Sanctions Policy** ("Policy") outlines the standards, requirements, and procedures the Company must follow to ensure adherence to these laws and to maintain a robust sanctions compliance framework.

Sanctions serve as a policy tool used by national governments and international bodies to deter threats to security, influence geopolitical behaviour, and uphold international norms. They are typically imposed in response to the actions of hostile nations, rogue regimes, transnational criminal groups, or broader global risks.

Although sanctions regimes differ in scope, enforcement mechanisms, and legal framework, they usually fall within one or more of the following categories:

- **Comprehensive Sanctions**

These broad measures target entire countries or geographic regions (e.g., the Crimea Region of Ukraine). They restrict nearly all forms of economic engagement, aiming to pressure governments by limiting access to financial systems, arms, goods, services, and other strategic resources.

- **Regime Based Sanctions**

These measures focus on specific governments or ruling authorities. They are typically list based and target individuals, officials, or entities associated with human rights abuses, corruption, or threats to national or international security. While tied to a particular country, they do not amount to a full trade embargo.

- **Sectoral Sanctions**

Sectoral sanctions target specific industries or economic sectors within a country. Although they allow for many routine business activities, they restrict transactions involving designated companies or segments critical to that country's strategic interests (e.g., energy, defence, finance).

- **Special Debt and Equity Sanctions**

These sanctions restrict targeted entities from issuing or trading new debt or equity. They allow day to day operations to continue but impede the ability to access longterm funding or investment. These measures often apply to entities within highimpact sectors or those owned or controlled by sanctioned governments.

- **Conduct Based Sanctions**

These sanctions focus on individuals or entities involved in specific types of illicit or harmful activities such as terrorism, proliferation of weapons of mass destruction, corruption, human rights abuses, organized crime, cybercrime, election interference, or drug trafficking. They are designed to identify, disrupt, and deter harmful conduct regardless of nationality or geographic location.

It is important to note that these sanctions categories are not mutually exclusive. A single sanctions regime may incorporate multiple components at once, depending on policy objectives.

### Sanctions Regimes Applicable to Aspro N.V.

Given the nature of the Company's operations, multiple international sanctions frameworks may apply to its Clients, transactions, products, and services. Below is an overview of the major regimes that directly affect the Company.

### 1. United Nations (UN)

Under Chapter VII of the UN Charter, the United Nations Security Council may impose sanctions to maintain or restore international peace and security. These sanctions are administered by Sanctions Committees and are aligned with FATF Recommendations 6 and 7.

UN Security Council resolutions are **legally binding** on all member states. Aspro N.V. complies with **all UN imposed sanctions** across its operations.

### 2. European Union (EU)

EU sanctions support the Common Foreign and Security Policy (CFSP), promoting peace, democracy, human rights, and international law. The EU:

- Implements all UN sanctions;
- May strengthen them with additional measures;
- May impose **autonomous sanctions** when deemed necessary.

EU sanctions apply:

- a) within EU territory and airspace;
- b) to all EU nationals, regardless of location;
- c) to all companies incorporated in an EU member state (including non EU branches);
- d) to any business conducted in whole or in part within the EU;
- e) on board EU jurisdiction vessels and aircraft.

Aspro N.V. complies fully with **all EU sanctions measures**.

### 3. United Kingdom (UK)

UK financial sanctions apply:

- a) within the UK and its territorial waters;
- b) to all individuals and entities operating in or from the UK;
- c) to UK nationals and UK incorporated entities worldwide, including non UK branches.

Aspro N.V. complies with **UK sanctions**, except where such compliance would conflict with EU law or other governing legislation.

### 4. United States (US)

US sanctions fall into two main categories:

#### • Primary US Sanctions

Binding on:

- US citizens and permanent residents
- All individuals and entities located within the US
- US incorporated entities and their foreign branches
- In some cases, foreign subsidiaries of US companies
- Foreign persons in possession of US origin goods (depending on the program)

#### • Secondary US Sanctions

These may apply **even to non US persons** operating entirely outside the US with no US nexus. Several OFAC programs include secondary sanctions, including those relating to Russia, Iran, and China/Hong Kong.

Aspro N.V. complies with **primary and, where legally permissible, secondary US sanctions**.

Where local law (e.g., EU blocking statutes such as Regulation (EC) 2271/96) prohibits compliance with certain secondary sanctions, the Compliance Officer must escalate the matter to the Director(s) and the Board for a decision.

## **Policy Statement**

Under this Policy, Aspro N.V. must:

- Block accounts or assets of sanctioned persons/entities where required by law.
- Prohibit or reject unlicensed transactions involving sanctioned individuals, entities, or jurisdictions.
- Terminate relationships with Clients confirmed to be sanctioned, unless local law prevents such action such circumstances must be escalated to the Director(s) and the Board.
- Refrain from engaging in or facilitating any arrangement structured to evade sanctions.

Failure to comply may result in severe consequences, including regulatory action, financial penalties, and reputational harm. Employees responsible for sanctions violations may face criminal liability, administrative fines, and disciplinary measures up to and including dismissal.

## **Roles and Responsibilities**

### **1. Board of Directors**

The Board is responsible for:

- Reviewing and approving this Policy periodically;
- Communicating the importance of sanctions compliance across the Company;
- Ensuring the Compliance function is adequately resourced, supported, and independent;
- Receiving and assessing regular sanctions and AML/CTF compliance reports;
- Appointing a qualified Compliance Officer with authority to escalate issues.

### **2. Director(s)**

Director(s) must:

- Review and assess compliance reports submitted by the Compliance Officer;
- Approve required changes or risk mitigation actions;
- Make final decisions on significant sanctions risks, conflicts of law, or escalated cases.

### **3. Compliance Officer**

Key responsibilities include:

- Conducting sanctions risk assessments on transactions and Clients;
- Reviewing documentary evidence provided by Clients;
- Recommending updates to this Policy and presenting them to the Board;
- Informing employees of sanctionsrelated changes, risks, and typologies;
- Ensuring Client identification information is complete and accurate.

#### 4. All Other Employees

Every employee is expected to:

- Comply with this Policy and all applicable sanctions laws;
- Remain vigilant and promptly report possible sanctions breaches;
- Avoid assisting or advising Clients on how to circumvent sanctions;
- Complete all required sanctions training;
- Never provide advice that could enable Clients to structure transactions to evade sanctions.

#### Sanctions Screening

The Company must conduct sanctions screening on all prospective and existing Clients, connected parties, third parties, and transactions. A specialized third party risk management system is used to ensure **ongoing screening** throughout the business relationship.

Screening results may include:

##### • True Positive

The applicant's information matches a sanctions/warning list entry exactly.

##### • Potential Match

Partial match due to limited data (e.g., missing date of birth), or the applicant is suspected of involvement in a crime.

##### • False Positive

The name matches a list entry, but further information confirms they are not the same person.

##### • Unknown

Insufficient information (e.g., single name provided) to confirm identity.

Cases marked **True Positive** or **Potential Match** are escalated to the Compliance Officer for further review.

If a Client is rejected based on screening results, they are assigned an appropriate rejection category, such as:

- Sanctions
- PEP
- Criminal Records
- Adverse Media

In case of positive matches against sanctions lists, the action performed by the Compliance Officer will be in line with the requirements of a specific sanctions program (e.g. asset freeze, rejection, or debt/equity restrictions etc.) as well in consideration with any potential conflict of law.

#### Sanctions Evasion

UN, U.S., and EU sanctions programs include prohibitions on evasion of their principal provisions, with authorities increasingly focusing on evasion as its own category of sanctioned activity. Examples of attempts to evade sanctions may include:

- Client (natural or legal person) who is not on any applicable sanctions list purchases cryptocurrency on behalf of a business entity owned by a sanctioned party.
- Where a payment is rejected by the Company, and the Client reissues the payment after changing or removing information, thereby making it difficult to identify and restrict payments to and from sanctioned parties or countries (activity known as “wire stripping”).
- Client physically located in the U.S. utilizes VPN to mask IP address, thereby making it possible to engage in a transaction that is permitted in the EU but prohibited for the US Persons; or
- Payments to a party who is located in a non sanctioned jurisdiction and acting as a “front company” or acting as an intermediary for sanctioned parties or parties in sanctioned jurisdictions.

Potential sanctions evasion activities may be detected by the Company’s staff at various levels of seniority and across different functions, i.e. through engagement with the existing or prospective Clients, business partners, transaction monitoring, ongoing due diligence (ODD) and other. All suspected attempts to evade or circumvent sanctions must be immediately escalated to the Compliance Officer who, after assessing the scenario, may decide that the case should be escalated to the relevant authorities.

In addition to sanctions screening, the Company utilizes its AML/CTF transaction monitoring, Client due diligence (CDD) and other processes to identify potential sanctions evasion activities by its Clients, third parties, and staff.

When performing the review and approval of Clients identified as high risk according to the Company’s ML/TF risk assessment methodology, the Compliance Officer also reviews the Client for potential sanctions evasion activities.

The results of the investigation shall be recorded in line with the Company’s AML Policy. Potential sanctions evasion activities, if detected, must be included in the AML/CTF and sanctions compliance reporting documents submitted by the Compliance Officer to the Executive Director(s) and the Board.

### **Asset Freezing**

For the purpose of this Policy, freezing, also known as “blocking”, refers to a form of controlling assets in which a sanctioned party has an interest. While title to blocked property remains with the sanctioned party, the exercise of the powers and privileges normally associated with ownership is prohibited without authorisation from the sanctioning competent authority. Blocking immediately imposes an across the board prohibition against transfers or transactions of any kind with regard to the property.

“Assets” refer to tangible or intangible resources with economic value that an individual, corporation or country owns or controls with the expectation that it will provide future benefit. In case of the Aspro N.V, the assets include cryptocurrency and fiat currency.

### **Sanctions Compliance Training**

Sanctions compliance training is one of the pillars of the Company's sanctions compliance programme. The Compliance Officer is responsible for reviewing and updating (where required) the sanctions compliance programme.

The compliance training falls under two categories:

1. Annual General Audience (All Staff) training,
2. Risk-based/Ad Hoc training to Staff who perform functions considered to be higher risk from a sanctions perspective, such as roles that entail Client contact, processing Client transactions, or otherwise evaluating Client data, must receive additional targeted training to supplement the annual sanctions learning provided to all Staff.

All Staff must receive annual General Audience (All Staff) sanctions compliance training. All new hires must receive the training within 30 (thirty) days of onboarding. The General Audience (All Staff) sanctions compliance training shall include, at a minimum:

- Major sanctions regimes (UN, EU, UK, US).
- Major sanctions programs and requirements.
- Sanctions evasion methods and techniques.
- Sanctions risk indicators ('red flags').
- Sanctions compliance roles and responsibilities of the Company's staff.
- Consequences of noncompliance.

All training records, including the training content (e.g. presentation slides, post course assessment) and attendance records must be kept in line with the recordkeeping requirements.

### **Outsourcing**

Where a sanctions compliance activity is outsourced to an entity outside the Company, the Company is ultimately accountable for ensuring that such activities are undertaken in compliance with the requirements of this Policy, and all applicable sanctions laws, rules and regulations.

### **Record-keeping And Record Retention**

The Company adopts one set of recordkeeping and record retention rules and requirements to all sanctions related items as set by the Company's AML Policy.

## **Appendix IV**

### **Client Acceptance Policy**

#### **Statement of the Policy**

Aspro N.V. has implemented this Customer Acceptance Policy ("CAP") to establish clear standards and procedures for assessing and approving customers who wish to access its online gaming and betting services. The purpose of this policy is to protect the company from being exploited for unlawful activities such as money laundering, terrorist or proliferation financing, sanctions evasion, fraud, and other illicit behavior, while ensuring full compliance with Curaçao's legal and regulatory framework.

This policy is aligned with the guidance of the Curaçao Gaming Control Board and forms part of Aspro N.V.'s wider Anti-Money Laundering (AML), Counter Terrorist Financing (CTF), and Counter Proliferation Financing (CPF) program. It also incorporates international best practices, including the Financial Action Task Force (FATF) Recommendations, the European Union Anti-Money Laundering Directives, and the Wolfsberg Principles.

To comply with Curaçao legislation, the policy integrates the requirements of the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance (SNO), the Kingdom Sanction Act, and the National Ordinance on Games of Chance (LOK).

This policy applies to all directors, officers, employees, contractors, and any third parties involved in onboarding and verification activities. No customer is allowed to deposit, withdraw, or engage in gaming activities until they have met all acceptance criteria and successfully completed the required identification, verification, and screening procedures.

## **2. Scope of the Policy**

This policy applies to every individual or entity that wishes to open an account with Aspro N.V., regardless of the registration channel used. This includes account creation through the company's official website, mobile applications, affiliate partnerships, or third party platforms.

The provisions of this policy cover the entire customer relationship, starting from the initial registration and continuing through all stages of account activity until closure or termination. It applies to all products and services provided by Aspro N.V. under its Curaçao gaming license OGL/2024/565/0553

## **3. Customer Acceptance Integration**

Aspro N.V. only accepts customers who meet all applicable legal, regulatory, and internal compliance requirements. Every applicant must be verified to confirm they have reached the legal age for gambling, which is at least eighteen (18) years or higher where required by the laws of their jurisdiction. Applicants are also required to provide accurate and verifiable personal details, including their full legal name, date and place of birth, nationality, and current residential address.

The company does not allow the registration of customers who are residents of, located in, or conducting transactions from jurisdictions restricted under Curaçao's regulatory framework, international sanctions regimes, or Aspro N.V.'s internal prohibited jurisdictions list. As part of the onboarding process, every applicant is screened against international and local sanctions lists, including those maintained by the United Nations, the European Union, the U.S. Office of Foreign Assets Control (OFAC), the U.K. Office of Financial Sanctions Implementation (OFSI), the Sanctions National Ordinance, the Kingdom Sanction Act, and any lists issued by the Curaçao Gaming Control Board.

All funds used for gaming and betting activities must come from legitimate, lawful sources. Where the company's risk assessment indicates the need for additional scrutiny, customers are required to provide supporting documentation to verify the origin of their funds and, if applicable, their source of wealth. Aspro N.V. also reserves the right to deny service to any individual or entity with a history of fraudulent behavior, chargebacks, bonus abuse, self exclusion due to problem gambling, or any other violation of gambling regulations.

#### **4. Risk-based Approach**

Aspro N.V. applies a thorough Risk-based Approach (RBA) during both the onboarding process and the ongoing assessment of its customers. This approach ensures that the level of due diligence applied is proportionate to the customer's individual risk profile. The evaluation takes into account a range of factors, including the customer's personal and financial background, the types of products and services they use, any geographic risks associated with their location or funding sources, and potential risks arising from the technologies or channels they use to access the platform.

##### **Customer Risk Profile**

Aspro N.V. assesses every prospective customer to determine their level of exposure to risks such as money laundering, terrorist financing, or proliferation financing. This assessment ensures that due diligence measures are applied proportionately to each customer's profile.

Customers who present clear, transparent, and verifiable financial backgrounds for example, those with stable employment in low risk sectors and gambling activity that aligns with their declared income are typically classified as low risk.

Conversely, customers may be considered high risk if they exhibit certain characteristics, such as having multiple or opaque income sources, employment in industries with elevated AML risk like cryptocurrency or unregulated financial services, or transaction patterns that appear inconsistent with their stated financial profile. Politically Exposed Persons (PEPs), their family members, and close associates are automatically categorized as high risk and are subject to stricter controls.

High risk cases are managed through Enhanced Due Diligence (EDD), which may include more detailed verification procedures, additional documentation requirements, and ongoing monitoring. Examples of high risk scenarios include:

- Customers with multiple or irregular income sources, who must provide evidence such as payslips, tax returns, business records, or investment statements.
- PEPs or their close associates, whose accounts require senior management approval, detailed source of wealth and source of funds checks, and ongoing enhanced monitoring.
- High or disproportionate spenders, where gambling activity exceeds what would reasonably match a customer's financial profile, requiring additional documentation and scrutiny.
- Customers exhibiting sudden, unexplained changes in gambling patterns or those using third parties to transact on their behalf, triggering immediate review and investigation.
- Attempts to operate multiple accounts, which are identified through internal monitoring systems and consolidated for a full transactional review.
- Unknown customers attempting to redeem large volumes of chips, or customers linked to junket operators, both of which require strict verification and EDD measures.

Aspro N.V. also conducts ongoing monitoring to ensure customer risk profiles remain accurate and up to date. Periodic reviews are scheduled, and additional checks are triggered whenever significant changes are detected, such as unusual transaction patterns, large unexplained deposits, or changes to a customer's personal or financial circumstances. Where risk levels increase, the company applies enhanced controls including EDD, closer transaction monitoring, or restrictions on account activity to ensure risks remain effectively mitigated and regulatory obligations are consistently met.

### **Geographic Risk Assessment**

Aspro N.V. uses a dynamic geographic risk framework to evaluate potential risks linked to a customer's location or the origin of their funds. This framework is regularly updated based on trusted and authoritative sources, including publications and lists from the Financial Action Task Force (FATF), the Caribbean Financial Action Task Force (CFATF), the European Commission's high risk country listings, the U.S. Office of Foreign Assets Control (OFAC), the U.S. Department of State's International Narcotics Control Strategy Reports, and Transparency International's Corruption Perceptions Index.

Customers from jurisdictions subject to international sanctions are not accepted under any circumstances. Those from high risk jurisdictions may be considered for onboarding only after Enhanced Due Diligence (EDD) is completed and senior compliance approval is granted.

Jurisdictions are considered high risk when they exhibit one or more of the following characteristics: inadequate Anti-Money laundering and counterterrorist financing frameworks or poor enforcement of such measures, systemic corruption that increases the likelihood of illicit funds entering the platform, association with international sanctions related to terrorism or weapons proliferation, or active presence of terrorist organizations.

To maintain accurate classifications, Aspro N.V. continuously monitors relevant global and regional sources. These include FATF high risk and monitored jurisdictions lists, CFATF advisories, the European Commission's list of countries with strategic AML/CFT deficiencies, OFAC sanctions lists, U.S. State Department reports, and corruption indices or reports indicating potential links to terrorist financing.

When a customer's country of residence or source of funds appears on a high risk or sanctioned list, the case is escalated to the Compliance Officer. In such instances, EDD measures are mandatory, including in depth identity verification, a thorough review of the source of funds and source of wealth, and enhanced transaction monitoring for as long as the relationship continues.

### **Geographic Risk Assessment Process**

1. **Initial Screening** – The customer's location and funding sources are checked against global lists and reports to determine their risk level.
2. **Low Risk Jurisdiction** – The account may be approved under standard due diligence procedures with routine monitoring.
3. **High risk Jurisdiction** – The application is escalated to compliance for review. Onboarding is only approved if all EDD criteria are satisfied, and heightened monitoring is applied.
4. **Sanctioned Jurisdiction** – The application is rejected, and records are retained in compliance logs.

5. **Ongoing Monitoring** – Customer profiles are dynamically updated, and additional controls are applied if jurisdictional risk changes over time.

### **Product, Service, and Transaction Risks**

The level of risk associated with a customer is also determined by the products, services, and transaction types they use. Certain activities naturally carry a higher degree of risk due to reduced transparency and traceability. Examples include peer to peer transfers, the purchase or exchange of gaming tokens, or the use of anonymous or semi anonymous payment methods such as prepaid cards or specific cryptocurrencies.

Accounts that are used mainly for financial transactions rather than genuine gameplay such as those making large deposits followed by minimal or no betting activity before withdrawals are treated with caution and subject to closer review. Likewise, the use of payment instruments not registered in the account holder's name automatically triggers additional verification measures to confirm legitimacy.

To mitigate these risks, Aspro N.V. actively monitors and manages several key risk areas. Funds deposited into gaming accounts must always originate from lawful and verifiable sources. If there are signs that funds may be linked to criminal activities such as fraud, theft, or trafficking, customers are required to provide evidence of the legitimate source of those funds, and any suspicious transaction is reported to the Financial Intelligence Unit (FIU) in line with legal requirements.

Anonymous or semi anonymous payment channels, including prepaid cards and certain virtual assets, are treated as high risk and subject to enhanced verification procedures, with full documentation of the source of funds. Accounts must also be used solely for genuine gaming purposes. Any behavior suggesting misuse, such as depositing and withdrawing without significant gameplay, triggers an immediate review and may lead to account suspension during investigation.

Transactions involving third party payment methods are flagged and subject to full verification of both the customer and the third party, including establishing the relationship between them and confirming the legitimacy of the funds. Similarly, transfers between gaming accounts are generally prohibited unless a legitimate and documented reason exists, in which case approval from the Compliance Officer is required, and full records of the transaction are maintained.

Operating multiple accounts or wallets including those on different platforms under the company's control is considered a red flag. Internal monitoring systems are designed to detect and link related accounts, ensuring consolidated oversight and the ability to conduct a thorough review of all connected activity. Customers who frequently change their payment methods or banking details may also be attempting to obscure the origin of funds; such patterns prompt a detailed profile review and, where appropriate, the application of Enhanced Due Diligence (EDD).

Aspro N.V. applies robust identity verification and authenticity checks to prevent and detect identity fraud. Any suspected cases are escalated to the relevant authorities in line with regulatory obligations. Additional controls are applied to the use of electronic wallets, particularly where providers are licensed in jurisdictions with weak AML or CTF oversight or where their structures make it difficult to trace funds. Customers using e-wallets are required to verify the source of their funds, and the provider's licensing and compliance standards are checked before any transaction is approved.

### **Channel and Technology Risk**

The level of risk associated with a customer also depends on the channels and technologies used to access Aspro N.V.'s services. Remote onboarding, while convenient, carries a higher risk of identity fraud or impersonation. To address this, the company relies on advanced digital Know Your Customer (KYC) solutions that include biometric verification, document authenticity checks, geolocation validation, and multifactor authentication.

Before introducing any new technologies, payment solutions, or platform features, Aspro N.V. conducts a comprehensive risk assessment to ensure the innovation cannot be misused for money laundering, fraud, or other illicit purposes.

Several factors are monitored closely to manage channel and technology related risks. Any method that allows customers to remain anonymous is considered high risk and triggers enhanced verification measures. These measures include identity document validation, biometric checks, and real time screening against sanctions and Politically Exposed Person (PEP) lists.

Remote interactions, although common in the industry and not inherently high risk, still demand strong safeguards. Aspro N.V. uses secure verification technologies such as biometric checks, liveness detection, and automated document validation to prevent impersonation and fraud during onboarding and transactions.

When third parties are involved in customer interactions, the risk profile increases, especially if the intermediary is not subject to AML/CFT obligations. In such cases, Aspro N.V. performs due diligence not only on the customer but also on the third party. This process includes verifying the intermediary's regulatory status, assessing its compliance framework, and ensuring all provided information is accurate and verifiable.

### **Risk Indicators**

Aspro N.V. applies a structured set of risk indicators to assess the level of risk associated with every customer relationship. These indicators form part of the company's Risk-based Approach (RBA) and ensure that the level of due diligence applied is always proportionate to the customer's overall risk profile.

The evaluation covers multiple categories:

- **Customer Risk Profile** – factors such as multiple or irregular income sources, Politically Exposed Persons (PEPs), high or disproportionate spending, sudden changes in spending behavior, involvement of third parties, multiple accounts, unknown chip redemptions, or links to junket operations.
- **Product, Service, and Transaction Risk** – warning signs such as proceeds of crime, anonymous or unregulated payment methods, misuse of accounts, third party funding, frequent changes in payment instruments, identity fraud, or the use of multiple e-wallets.

- **Geographic Risk** – customers connected to jurisdictions with weak AML/CFT frameworks, high levels of corruption, international sanctions, terrorism links, or countries listed by FATF, CFATF, OFAC, or Transparency International's CPI.
- **Channel and Technology Risk** – customers accessing services through anonymous or unverified channels, onboarding remotely without sufficient identity validation, or relying on unregulated third party intermediaries.

To determine the customer's overall risk, the company uses an internal Risk Calculator that assigns a weighted score to each indicator. The total score determines the customer's classification:

| Risk Level         | Requirements                                                                                                                                    |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Low Risk</b>    | Standard Customer Due Diligence (CDD) applies, with documentation limited to what is legally required or triggered by a change in risk profile. |
| <b>Medium Risk</b> | Standard CDD plus additional verification steps and closer ongoing monitoring.                                                                  |
| <b>High Risk</b>   | Full Enhanced Due Diligence (EDD), senior management approval prior to onboarding, and enhanced ongoing monitoring.                             |

This riskscoring approach ensures a consistent and methodical assessment of customers, allowing the company to allocate its resources effectively and meet its regulatory obligations.

### Guidance on Using the Risk Indicators

These indicators are designed to help staff assign an accurate risk profile to each customer during onboarding and throughout the customer relationship. Each factor should be assessed individually, and the combined results should inform the overall risk classification.

- Customers with mostly low risk indicators are assigned a low risk profile and subject to standard Customer Due Diligence (CDD).
- Customers with a mix of low and medium risk indicators are classified as medium risk and require additional verification and closer monitoring.
- Customers displaying one or more high risk indicators must undergo Enhanced Due Diligence (EDD), senior management approval before onboarding, and ongoing heightened monitoring.

Risk profiles should be reviewed regularly and adjusted when customer behavior, transaction patterns, or external risk factors change. This approach ensures that the company's risk management remains dynamic and aligned with regulatory expectations.

## 5. Onboarding Procedures

Aspro N.V. follows a structured and well documented onboarding process to ensure that only customers meeting the company's acceptance standards gain access to the platform. No account is activated until the customer has successfully completed all required identification, verification, and sanctions screening steps.

During registration, customers are required to provide their full legal name, date and place of birth, nationality, residential address, and an official identification number such as a passport or national ID.

Every applicant is screened against international sanctions and Politically Exposed Person (PEP) databases using automated tools to ensure comprehensive coverage. Any potential matches or alerts are reviewed manually by trained compliance officers to confirm accuracy and rule out false positives.

If a customer is identified as high risk during the initial assessment, additional verification is required. This includes providing documentation to confirm the legitimacy of their funds and, where relevant, the source of their wealth. Acceptable documents may include recent bank statements showing income deposits, business account records or financial statements, tax returns, contracts of property or asset sales, and investment account statements. These enhanced measures ensure that the company meets regulatory expectations and maintains a strong control framework to protect the platform from misuse.

### **Client Identification requirements and verification procedures**

This section refers to individuals who directly or indirectly establish a business relationship with the Company (e.g. direct Clients, beneficial owners, authorized persons, etc.). The Company should be satisfied that it is dealing with a real person and obtain sufficient evidence of identity to establish that a prospective Client is who he/she claims to be.

### **Document verification is intended to prevent the following issues:**

Forgery  
Data tampering  
Photo replacement  
Fraud  
Using document printouts  
Other manipulation

### **The ID document must contain as minimum the following information:**

Owner full name  
Owner full date of birth  
Document number  
Validity data (issue date or validity period)  
Owner photo  
Owner signature (if applicable)

The ID document should meet the following requirements:

- The document is valid for at least one month from the upload date.

- The document is not scratched, stained, or torn.
- The applicant full name, date of birth and other important information is present and can be read.

### Uploading the photo of an ID document

The photo of the ID document uploaded to the system should meet the following requirements:

The uploaded file is an original photo (static image) or scan (not a screenshot or a photo uploaded from social networks) in JPG, JPEG, PNG, PDF.

If the document has data on the front and back, both sides should be uploaded.

The size of the uploaded file is no less than 100 KB or 300 DPI.

The photo is in colour.

The information in the document is readable.

All corners of the document are visible and no foreign objects or graphic elements are present.

The uploaded photo has not been edited with any software or converted to PDF.

The document is not digital (in most cases).

### Checking the image for authenticity

The image authenticity check is intended to ensure that the uploaded image has not been edited electronically. This process involves automated signature analysis.

A software signature includes file metadata, compression parameters, vendor or softwarespecific tags, sections, and so on. An extensive database of camera and software signatures are utilized to determine the source of an image, detect traces of modification software, and estimate the risk of intended image tampering (as opposed to cosmetic changes like cropping, resizing, or rotation).

### Document data validation

At the final step, the data extracted from the document is checked against various sources, including sanctions and watchlist databases.

#### **1. Proof of address verification**

##### **a. Face-to-face procedures**

For the purpose of face face Client identification, the Compliance Officer shall inspect the person's original Proof of Address (PoA) documentation and make a certified true copy to be maintained as evidence of verification.

##### **b. Nonface to face procedures**

The process of Proof of Address (PoA) document verification for nonface to face Clients consists of the following steps:

- **Uploading a PoA photo.**

By default, the system accepts PoA documents that have been issued within the last 3 months.

- **Checking the image for authenticity.**

The image authenticity check is intended to ensure that the uploaded image has not been edited electronically. This process involves automated signature analysis.

A software signature includes file metadata, compression parameters, vendor or software specific tags, sections, and so on. An extensive database of camera and software signatures are utilized to determine the source of an image, detect traces of modification software, and estimate the risk of intended image tampering (as opposed to cosmetic changes like cropping, resizing, or rotation).

Each image receives a digital trust score:

- Low – red (high risk of editing).
- Acceptable – yellow (there might be something to take a closer look at).
- Normal – green (a trusted and authentic image).

- **Checking the integrity of the image.**

Integrity checks are designed to ensure the uploaded image represents an official document by comparing it with a template from a database of original documents. Integrity checks consist of:

- General conformity to the template.
- Font originality and compliance with the relevant standards (width, spaces between the letters, and so on).
- Required fields and inscriptions.
- Data extraction (full name, home address, issue date).
- Data validation (whether the address is complete, if it exists and if it is really a home address).

To ensure the completeness and consistency of the extracted address data, external map services, such as Google Maps, Open Street Map, and others, are utilized allowing the Compliance Officer to see the applicant's geolocation in the Dashboard.

## **Supported PoA Documents**

Common proof of residency examples:

- Tax bill (not older than 3 months).
- Mortgage statement.
- Certificate of voter registration.

- Correspondence with a government authority regarding the receipt of benefits such as a pension, unemployment benefits, housing benefits, and so on.
- Cable internet/TV bill (but not from satellite TV companies or for other wireless telecommunication services).
- Landline telephone bill.
- Bank statement with the date of issue and the name of the person (the document must be not older than 3 months).
- Utility bill for gas, electricity, water, internet, etc. linked to the property (the document must not be older than 3 months).
- A lease agreement that is current and has the signatures of the landlord and the tenant.
- Rent bills issued by a real estate rental agency.
- Credit card statement issued by a bank.
- Letter from a recognized public authority or public servant (any government issued correspondence not older than 3 months).
- Employer's certificate for PoA.
- House purchase deed.
- The document must contain the full name, home address, and the document issue date (in most cases). Both paper documents and electronic documents (in PDF) are accepted.

### **Alternative proof of residency examples**

The following documents can also be accepted as valid PoA, but only if they contain an address:

- Passport
- Identity card
- Driving license
- Residence permit (EU samples containing address)

*\*\*\* The same document cannot be used to confirm both an identity and a place of residence. So, if an applicant submits an ID document as PoA, they should use another document to confirm their identity.*

### **Documents which are not acceptable as Proof of Address, include:**

- Old government issued correspondence (older than 3 months)
- Old bank statements (older than 3 months)
- Old utility bills linked to the property (older than 3 months)
- Pension statements
- Bank references
- Insurance policies
- Mobile phone bills
- Medical bills

- Receipts for purchases
- Insurance statements
- Documents stating PO Box addresses
- Checks
- Envelopes and parcels showing your name and an address
- Prepaid card invoices
- Mobile sim cards+ bills issued to a business address
- Bills from debt collection agencies
- Bills from fintech companies
- Papers referring to discount cards which cannot be considered as bank cards
- Car rent bills

### **Source of Funds (SoF) and Source of Wealth (SoW)**

SoF refers to origin of funds being deposited, received, or transferred with the Company. SoF tells us where the money is coming from, which can be proven through bank statements, tax returns or the Company financials, etc.

Typically, SoW is requested when establishing business relationships or performing EDD, SoF is requested when there is a need to understand what the origin of a transaction is.

Examples of SoW and SoF and supporting documentation that can be provided, include:

| Income category                                                                  | Documents required                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Income from salary                                                               | <ul style="list-style-type: none"> <li>• Pay slips for the past 3 months and bank statement showing the salary being paid into this bank account;</li> <li>• Audited personal tax statement.</li> </ul>                                                                                                                                                                                                                                                                                                   |
| Inheritance                                                                      | <ul style="list-style-type: none"> <li>• Grant of Probate (with a copy of the Will) clearly showing the amount of inheritance and a bank statement showing these funds being deposited into the account;</li> <li>• Signed letter from a licensed solicitor or estate trustees on letterheaded paper clearly indicating the amount of inheritance, accompanied by updated proof of the solicitor's regulated status and a bank statement showing these funds being deposited into the account.</li> </ul> |
| Gift/donation                                                                    | <ul style="list-style-type: none"> <li>• Notarized gift/ donation letter and a bank statement showing these funds being deposited into the account;</li> <li>• Gift agreement and a bank statement showing these funds being deposited into the account.</li> </ul>                                                                                                                                                                                                                                       |
| Savings/deposits                                                                 | <ul style="list-style-type: none"> <li>• Savings statement;</li> <li>• Bank statement.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                         |
| Government grants (retirement income, grants for veterans, research grant, etc.) | <ul style="list-style-type: none"> <li>• Type of received grant and a bank statement showing these funds being deposited into the account;</li> <li>• Documents confirming/ proving received grant and a bank statement showing these funds being deposited into the account.</li> </ul>                                                                                                                                                                                                                  |
| Company profit / dividends                                                       | <ul style="list-style-type: none"> <li>• Dividend contract note or equivalent and a bank statement showing these funds being deposited into the account;</li> <li>• Copy of latest audited financial statements;</li> <li>• Tax declaration form.</li> </ul>                                                                                                                                                                                                                                              |
| Loan or investment                                                               | <ul style="list-style-type: none"> <li>• Loan/Investment agreement or other documents confirming the agreement and a bank statement showing these funds being deposited into the account.</li> </ul>                                                                                                                                                                                                                                                                                                      |

|                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Sales (of property, goods, shares, etc.)</p> | <ul style="list-style-type: none"> <li>• Copy of contract of buy/sale/production and a bank statement showing these funds being deposited into the account;</li> <li>• Prove of eshop sale report (screenshot) with the list of items sold and a bank statement showing these funds being deposited into the account;</li> <li>• Shipping documents and a bank statement showing these funds being deposited into the account;</li> <li>• Proof of delivery and a bank statement showing these funds being deposited into the account;</li> <li>• Customs declaration;</li> <li>• Audited financial report;</li> <li>• Tax report;</li> <li>• Statement evidencing the money and a bank statement showing these funds being deposited into the account.</li> </ul> |
|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### **Ongoing Monitoring**

Aspro N.V. recognizes that customer acceptance is an ongoing process rather than a onetime activity. Continuous monitoring is essential to ensure that customer behavior remains consistent with the profile established during onboarding and that any irregularities or deviations are promptly identified and addressed.

The company uses automated transaction monitoring systems to detect patterns of unusual or suspicious behavior. Alerts are generated for activities such as deposits or withdrawals that do not match the customer's declared profile, rapid movement of funds without meaningful gameplay, the use of multiple or unusual payment methods, or patterns that may suggest collusion, chip dumping, or other prohibited activities.

Each alert is reviewed by trained compliance officers, who assess the circumstances and determine whether further investigation or escalation is needed.

In addition to real time monitoring, the company conducts periodic reviews of customer profiles on a risk-based schedule to ensure risk ratings remain accurate. If there are material changes in a customer's situation, such as relocation to a high risk jurisdiction, significant increases in transaction values, or changes in funding methods, the customer's risk profile is immediately reassessed. Where necessary, enhanced monitoring and other controls are applied to maintain compliance and mitigate potential risks.

### **Prohibited clients and transactions**

Certain types of Client/transactions are not accepted for establishing business relationships or conducting transactions in order to reduce the risk that the services and products of the Company may be used for money laundering or terrorist financing or other illicit purposes and at the same time for protect the Company from the financial, reputational and legal risks.

Consequently, it is strictly prohibited to:

- c. Establish a business relationship with Clients who fail or refuse to submit the requisite data and information for the verification of their identity and the creation of their economic profile, without adequate justification.

- d. Establish a business relationship and/or conduct transactions with natural or legal persons against which sanctions prohibiting such relationship/transactions are imposed in accordance to the Company's Sanctions Policy (Appendix II).
- e. Conclude or implement any business relationship with a credit institution or other financial institution or an institution that carries out activities equivalent to those carried out by credit institutions and financial institutions or legal person that is incorporated in a jurisdiction in which it has no physical presence, involving meaningful management and which is unaffiliated with a regulated financial group (i.e. shell company) or is known to permit accounts to be held by a shell bank.
- f. Establish a business relationship or conduct transactions that involve in any way, directly or indirectly, natural or legal persons whose activities are related to criminal activity including (but not exhaustive)
- Terrorist offences, offences related to a terrorist group and offences related to terrorist activities as set out on Titles II and III of Directive (EU) 2017/541 (replacing Framework Decision 2002/475/JHA on combating terrorism)
  - Any of the offences referred in article 3(1)(a) of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances;
  - The activities of criminal organizations as defined in Article 1(1) of Council Framework Decision 2008/841/JHA on the fight against organized crime;
  - Trafficking in human beings and migrant smuggling, including any offence set out in Directive 2011/36/EU;
  - Sexual exploitation, including any offence set out in Directive 2011/93/EU;
  - Fraud affecting the Union's financial interests, where it is at least serious, as defined in Article 1 (1) and Article 291) of the Convention on the protection of the European Community's financial interests;
  - Corruption, including any offence set out in the Convention on the fight against corruption involving officials of the EU Communities or officials of Member States of the EU;
  - All offences, including tax crimes relating to direct taxes and indirect taxes and as defined in the national Laws of Lithuania and which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, if there is a legal threshold by Law for such offences, all offences punishable as above for a minimum of more than six months;
  - Counterfeiting of currency, including any offence set out in Directive 2008/99/EC;
  - Cybercrime, including any offence set out in the Directive 2013/40/EU;
- g. Establish a business relationship or conduct transactions that involve in any way, directly or indirectly, natural or legal persons where:

- Legal entities are owned through bearer instruments;
  - Legal entities are involved in the adult industry;
  - Legal entities are involved drugs industry;
  - Legal entities are involved in arms industry;
  - Specially Designated Nationals and Blocked Persons (SDNs);
  - Clients acting on behalf of Specially Designated Nationals and Blocked Persons (SDNs);
  - Clients whose source of funds (SoF) and source of Wealth (SoW) were generated from a sanctioned activity;
  - Clients whose source of funds (SoF) and source of Wealth (SoW) cannot be verified when this is required;
  - Purchase or sale of virtual assets ultimately owned or controlled, directly or indirectly, by sanctioned parties;
  - Transactions with third parties ultimately owned or controlled, directly or indirectly, by sanctioned parties;
- h. Establish a business relationship and/or conduct transactions with natural or legal persons residing in a jurisdiction/country where it is prohibited by Company policy to offer its services to. Prohibited jurisdictions / countries shall include:

#### Unrecognised / Disputed Territories

|                                             |                                     |
|---------------------------------------------|-------------------------------------|
| Crimea                                      | Republic of Abkhazia                |
| Donetsk                                     | Republic of China (Taiwan)          |
| Luhansk                                     | Republic of Kosovo                  |
| Nagorno Karabakh Republic                   | Republic of Somaliland              |
| Palestine                                   | Republic of South Osetia            |
| Pridnestrovian Moldavian Republic           | Turkish Republic of Northern Cyprus |
| <b>Prohibited Jurisdictions / Countries</b> |                                     |
| Australia                                   | Libya                               |
| Belarus                                     | Mali                                |
| Belize                                      | Netherlands                         |
| Central African Republic                    | North Korea                         |
| Cuba                                        | Russia                              |
| Curaçao                                     | Somalia                             |
| Democratic Republic of Congo                | Sudan                               |
| Dutch West Indies (Aruba, Bonaire)          | Syria                               |
| France                                      | Turkish Republic of Northern Cyprus |
| Germany                                     | UK                                  |
| Iran                                        | USA                                 |
| Iraq                                        | Yemen                               |
| Lebanon                                     | Libya                               |

## **Enhanced Due Diligence (EDD)**

Enhanced Due Diligence (EDD) procedures are applied to customers who present an elevated risk profile. This includes Politically Exposed Persons (PEPs), their family members, and close associates; customers based in or funding their accounts from high risk jurisdictions; those conducting unusually large, complex, or unexplained transactions; and customers whose financial behavior is inconsistent with their declared income or business activities.

EDD involves a more detailed and rigorous verification process than standard due diligence. This includes a full analysis of the customer's source of funds and source of wealth, supported by credible and independent documentation. Additional steps include corporate registry and public record searches to verify legal and beneficial ownership, confirmation of employment or business ownership, reviews of audited financial statements or other reliable financial documents, and thorough adverse media and reputational checks.

Senior management approval is required before onboarding any high risk customer, and in complex or sensitive cases, formal approval from the Board of Directors may be necessary.

Once these customers are onboarded, they are subject to ongoing enhanced monitoring. This includes lower thresholds for triggering transaction reviews, closer scrutiny of their transaction patterns, and more frequent reassessments of their risk profiles. These measures ensure that higher risk relationships are managed appropriately, in full alignment with both regulatory obligations and the company's internal risk appetite.

### **Prohibited Customer Categories**

Aspro N.V. will not onboard or will immediately terminate relationships with customers who meet any of the following criteria:

- Anonymous or unverifiable customers, including those who fail or refuse identity verification within 30 days.
- Shell companies, fictitious entities, or customers with unclear beneficial ownership.
- Sanctioned individuals or entities, including those appearing on UN, EU, OFAC, OFSI, SNO, or Kingdom Sanction Act lists.
- Residents of or transacting from prohibited or sanctioned jurisdictions, as defined in Section 4 (Geographic Risk).
- Customers below the legal age for gambling.
- Customers involved in fraud, bonus abuse, identity theft, or other illicit behaviour.
- Third party transactors or users of anonymous payment channels without valid justification or verification.
- Customers whose source of funds or source of wealth cannot be verified or is linked to crime.

### **Acceptance and Rejection Triggers**

Customer applications will be immediately rejected or suspended when any of the following triggers occur:

a. Documentation and Verification Failures

- Refusal to provide KYC, proof of address, or EDD documentation.
  - Submission of false, altered, or misleading information.
  - Failure to complete mandatory verification within 30 days.
- b. AML/CTF/CPF Risk Triggers
- Positive sanctions match or verified PEP hit without manageable risk.
  - Suspicion of money laundering, terrorist financing, proliferation financing, or other criminal activity.
  - Inability to verify SOF/SOW after reasonable attempts.
- c. Behavioural and Transactional Triggers
- Highly unusual deposit/withdrawal activity inconsistent with profile.
  - Multiple accounts, third party payments, or misuse of payment instruments.
  - Attempts to circumvent controls or operate through intermediaries.
  - Evidence of collusion, chip dumping, or nongenuine gameplay.

## Termination

Aspro N.V. reserves the right to suspend or terminate any customer relationship when required by regulations, internal policies, or risk considerations. This action may be taken if a customer fails to provide the requested identification or supporting documentation within 30 calendar days, if there is reasonable suspicion of money laundering, terrorist financing, or proliferation financing, or if the customer engages in activities that violate applicable laws, regulations, or the company's Responsible Gambling Policy.

When a relationship is terminated due to suspected criminal activity, the company promptly files a report with the Financial Intelligence Unit (FIU) in accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT). Any remaining funds in the account are returned to the original funding source unless there is a legal requirement to freeze or seize the funds pending investigation. Detailed records of all termination actions, including the rationale and supporting evidence, are maintained for at least five years.

Aspro N.V. will refuse to onboard or will terminate an existing relationship in cases where:

- The customer is a resident of, located in, or conducting transactions from a prohibited or sanctioned jurisdiction.
- The customer fails to provide required information or documentation within the specified timeframe.
- False, misleading, or incomplete information is provided during registration or verification.
- The source of funds or source of wealth cannot be confirmed as legitimate.
- The customer is involved in, or suspected of, money laundering, terrorist financing, or other criminal activity.
- The customer is a Politically Exposed Person (PEP) whose risk profile cannot be mitigated to an acceptable level. Fraudulent activities, bonus abuse, collusion, or prohibited gambling behavior are detected.
- The customer attempts to use third parties to transact without proper disclosure and verification.

- The customer has self excluded or been excluded for responsible gambling reasons.
- Large chip redemptions or withdrawals are requested without verifiable linked gambling activity.
- The customer is a minor or below the legal gambling age in their jurisdiction.

### **Curaçao's Legislative Framework**

Aspro N.V. acknowledges that its Customer Acceptance Policy is an integral part of its wider Anti-Money Laundering (AML), Counter Terrorist Financing (CTF), and Counter Proliferation Financing (CPF) framework. The policy is designed to fully comply with Curaçao's legal and regulatory requirements, including the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance (SNO), the Kingdom Sanction Act, and the National Ordinance on Games of Chance (LOK).

Compliance with these obligations is treated as a priority in daily operations. The customer acceptance procedures are embedded within the company's compliance processes to ensure due diligence is continuous and extends beyond onboarding. This approach ensures that any significant changes in a customer's risk profile, transactional behavior, or jurisdiction are identified and addressed promptly.

All employees involved in onboarding and verification activities receive dedicated training to help them understand the legislative framework and the company's internal standards. The training focuses on effectively applying the Risk-based Approach, identifying and escalating high risk indicators, and following escalation protocols to the Compliance Officer or senior management.

Independent audits are conducted at least annually to evaluate how effectively the Risk-based Approach and the Customer Acceptance Policy are being implemented. These audits review critical processes, such as identity verification, sanctions and PEP screening, Enhanced Due Diligence (EDD) procedures, and the ongoing monitoring of customer activities. The findings are reported to the Board of Directors, and any gaps or deficiencies are addressed promptly through corrective measures implemented within defined timeframes.

## **11. Responsible Gambling Integration**

Aspro N.V. ensures that its Customer Acceptance Policy is fully aligned with its Responsible Gambling Policy, recognizing that protecting customers from gambling related harm is a key part of its compliance and operational framework.

If a customer shows behavior that indicates potential harm, such as frequent deposits that exceed their apparent financial capacity or excessively long gaming sessions, the company takes immediate action. Depending on the situation, this may include setting deposit or wagering limits, temporarily suspending the account, or, in severe cases, refusing further access to services to protect the customer.

Self exclusion requests are handled promptly and applied to all accounts linked to the customer to ensure these measures cannot be bypassed. These restrictions remain active for the period specified by the customer or as required by regulatory standards.

Employees in customer facing roles receive targeted training to help them identify early signs of problem gambling. This training is incorporated into both the onboarding process and ongoing monitoring activities, enabling timely intervention when risk indicators are observed.

#### **Review and Governance of CAP**

This Customer Acceptance Policy (CAP) is reviewed at least once every twelve months to ensure that it remains effective, compliant with legislative and regulatory requirements, and consistent with industry best practices. The review process also takes into account any changes to the company's risk profile, emerging patterns in customer behavior, and technological advancements that could create new risks or vulnerabilities.

Proposed revisions or updates are prepared by the Compliance Officer and submitted to the Board of Directors for approval prior to implementation. All updates are thoroughly documented, and relevant staff are informed and trained to ensure that the revised policy is applied consistently and accurately throughout the company's operations.

#### **Record Keeping**

Aspro N.V. keeps detailed records of all customer acceptance activities for at least five years after the end of the business relationship, in accordance with regulatory requirements. These records include identification and verification documents, proof of address, evidence of the source of funds and source of wealth, transaction monitoring alerts and investigation reports, Enhanced Due Diligence (EDD) files, internal compliance reviews, and documentation of any account suspensions or terminations.

All records are stored securely in encrypted formats with strict access controls to ensure confidentiality and data protection. Only authorized personnel have access to these records, and all access activity is logged and periodically reviewed to verify compliance with internal policies and applicable data protection regulations.