

Money Laundering Prevention Manual for Companies in the iGaming Sector.

NovaWave Technology N.V., a limited liability company duly registered with the Curaçao Chamber of Commerce & Industry under registration number 162293, with its registered address at Schottegatweg Oost 10, Unit 1-9, Bon Bini Business Center, Curaçao.

01/2026

Irati Aparecida Santos, Compliance Officer.

1. Introduction

Purpose of the manual

Importance of Anti-Money Laundering (AML) in the iGaming sector

Document structure

iGaming Industry Overview

Description of the iGaming sector

Relevant regulations and regulatory bodies

Main risks of money laundering in iGaming

3. AML Policies and Procedures

Company commitment to AML

Designation of a person responsible for AML2. iGaming Industry Overview

Description of the iGaming sector

Relevant regulations and regulatory bodies

Main risks of money laundering in iGaming

Specific legal and regulatory requirements

4. Customer Knowledge (KYC)

Identity verification processes

Reliable sources of information

Continuous monitoring of customers and transactions

5. Due Third Party Diligence

Assessment of business partners and suppliers

Contracts and agreements that include AML clauses

6. Transaction Monitoring and Control

Tools and technologies used for monitoring

Warning indicators for suspicious transactions

Procedures for reporting suspicious transactions to authorities

7. Training and Awareness

AML Training Programs for Employees

Regular updates on regulations and best practices

8. Audit and Internal Review

Internal audit processes for compliance with AML policies

Periodic reviews of policies and procedures

9. Risk Management

Assessment and mitigation of risks specific to the iGaming sector

Strategies for dealing with new types of threats

10. Documentation and Registration

Maintaining adequate records of AML transactions and procedures

Secure storage and confidentiality of documents

11. Examples and Practical Cases

Case studies of money laundering incidents in the iGaming sector

Examples of best practices and common mistakes to avoid

12. Attachments

a) Glossary of terms related to AML

b) Regulatory and legislative references

c) KYC form templates

1. Introduction

The introduction of the Anti-Money Laundering (AML) Manual for companies in the iGaming sector sets the stage and defines the fundamental purpose of this document crucial to the operational and regulatory integrity of the company. This manual aims to provide clear guidelines and robust procedures to mitigate the risks associated with money laundering and terrorist financing within the specific context of iGaming activities.

Purpose of the Manual

The main objective of this manual is to guide all company operations in the iGaming sector, ensuring that all activities are aligned with Anti-Money Laundering (AML) best practices. It serves as a comprehensive guide to help the company implement effective policies and procedures that not only comply with local and international regulatory requirements, but also protect the organization's financial integrity against potential abuse and illegal practices.

Importance of Anti-Money Laundering (AML) in the iGaming sector

The importance of AML in the iGaming sector cannot be underestimated due to the nature of the activities involved. iGaming, which includes online casino games, sports betting, and other forms of digital entertainment, handles large volumes of financial transactions and fund movements. This creates an environment prone to being exploited by malicious individuals seeking to use iGaming platforms to launder illicitly obtained money.

Furthermore, the iGaming sector is often the target of strict regulations due to its potential impact on the economy, consumers' financial security and sporting integrity. Therefore, ensuring compliance with AML guidelines not only protects the company against severe legal penalties, but also promotes a reputation of trust and transparency with customers, investors and regulatory authorities.

Document Structure

The structure of this document follows a systematic approach to address all essential aspects of Anti-Money Laundering in the context of iGaming. It includes:

Introduction: Presentation of the purpose and importance of the manual.

iGaming Sector Overview: Contextualization of the specificities of the sector and the challenges faced in relation to AML.

AML Policies and Procedures: Detailing internal policies and operational procedures to ensure compliance with regulations.

Customer Knowledge (KYC): Discussion of methods for verifying customers' identities and monitoring their transactions.

Due Third-Party Diligence: Assessment of business partners and suppliers to mitigate AML risks.

Transaction Monitoring and Control: Use of technologies and processes to detect suspicious activities.

Training and Awareness: Implementation of educational programs for all employees.

Internal Audit and Review: Procedures to ensure the continued effectiveness of AML policies.

Risk Management: Strategies to identify and mitigate sector-specific risks.

Documentation and Recordkeeping: Maintaining detailed and secure records.

Examples and Practical Cases: Illustration of real situations and best practices in AML.

Attachments: Inclusion of document models and regulatory references.

This comprehensive framework not only guides the company in implementing effective preventative measures against money laundering, but also establishes a standard of compliance that reinforces the integrity and security of iGaming operations .

iGaming Industry Overview

Description of the iGaming sector

iGaming sector encompasses a variety of gaming activities carried out over the internet, including online casinos, sports betting, online poker, and digital lotteries. These platforms offer users the opportunity to participate in real-time gambling and betting, accessible from mobile devices and computers connected to the internet. The iGaming sector has grown significantly due to increased global digital connectivity and the convenience offered to players, allowing them to participate in games from anywhere at any time.

Relevant regulations and regulatory bodies

iGaming is a highly regulated sector due to the risks associated with online gambling, including concerns about consumer safety, sports integrity and Anti - Money Laundering (AML). Regulations vary significantly by jurisdiction, with some countries choosing to ban online gambling completely, while others implement a strict regulatory regime to control and monitor operations.

Regulatory bodies play a crucial role in overseeing iGaming activities and enforcing laws and regulations. Examples of regulatory bodies include the Malta Gaming Authority (MGA) in Malta, the United Kingdom Gambling Commission (UKGC) in the United Kingdom, the Directorate General for Gambling Regulation

(DGOJ) in Spain, and the Gambling Authority in Spain. Kahnawake in Canada, among others. These regulatory bodies are responsible for issuing licenses to iGaming operators, ensuring compliance with ethical and safety standards, and investigating irregularities or violations of established regulations.

Main risks of money laundering in iGaming

iGaming poses a number of specific money laundering risks due to the nature of the financial transactions and the anonymity potentially afforded to users. Some of the main risks include:

Anonymity and use of cryptocurrencies: Transactions carried out on iGaming platforms can be conducted anonymously, especially when cryptocurrencies are used as a means of payment, making it difficult to identify the final beneficiaries.

iGaming operators can be targets for money laundering, where illicit funds are mixed with legitimate winnings before being removed from the platform.

Complexity of ownership structures: Some iGaming operators may utilize complex corporate structures or those located in offshore jurisdictions to hide the true origin of funds or ultimate beneficiaries, making it difficult to identify suspicious transactions.

Compliance with fragmented regulations: Due to the diversity of global regulations, iGaming operators can face significant challenges when trying to comply with the regulatory requirements of multiple jurisdictions simultaneously, creating potential loopholes for money laundering activities.

Understanding these risks allows iGaming operators to implement robust preventative measures, such as conducting due appropriate customer and transaction due diligence, continuous monitoring of suspicious activity, and effective cooperation with regulatory bodies to effectively mitigate money laundering risks in the sector.

3. AML Policies and Procedures

Company commitment to AML

The company's commitment to Anti-Money Laundering (AML) is critical to ensuring integrity and compliance in iGaming operations. AML is not only a regulatory requirement, but also an essential ethical pillar that demonstrates corporate responsibility and protects the interests of customers and stakeholders. By adopting robust AML policies and procedures, the company not only complies with regulations imposed by regulatory bodies, but also strengthens its reputation as a reliable and ethical operator in the iGaming sector.

Designation of an AML person

Designating an AML person is crucial to ensuring that all Anti-Money Laundering initiatives and policies are implemented effectively and consistently. This individual, often referred to as the Compliance Officer or the AML Officer, has the responsibility for leading and overseeing AML-related activities within the company.

The main responsibilities of the AML person include:

Policy Develop and regularly update AML policies and procedures that are aligned with current regulations and industry best practices.

Implementation of Internal Controls: Ensure that effective internal controls are established to mitigate money laundering risks, including due diligence procedures customer due diligence, transaction monitoring and suspicious activity reporting.

Training and Awareness: Coordinate AML training programs for employees at all levels of the organization, ensuring everyone understands their responsibilities and legal obligations.

Monitoring and Auditing: Carry out continuous monitoring of the company's activities to identify and investigate suspicious transactions, in addition to conducting periodic audits to evaluate the effectiveness of AML controls.

Relationship with Regulators: Maintain an open and cooperative dialogue with regulatory bodies and competent authorities, providing necessary information and promptly responding to compliance requests.

The presence of a dedicated AML officer not only strengthens the company's commitment to regulatory compliance, but also provides an effective line of defense against potential money laundering threats in the iGaming sector .

Specific legal and regulatory requirements

Specific legal and regulatory requirements in the iGaming sector vary significantly by jurisdiction. However, there are common guidelines that iGaming operators must follow to ensure compliance with AML regulations:

Identity Verification: Establish robust Know procedures Your Customer (KYC) to verify the identity of customers and ensure that they are not used by individuals or entities involved in illicit activities.

Transaction Monitoring: Implement continuous transaction monitoring systems to identify unusual patterns of activity that may indicate money laundering or terrorist financing.

Reporting Suspicious Activity: Establish clear procedures for reporting suspicious activity to appropriate authorities, as required by local and international laws.

AML Training: Ensure all employees are regularly trained in AML to recognize signs of suspicious activity and comply with established policies and procedures.

Audit and Review: Conduct regular internal audits to assess the effectiveness of AML controls and ensure ongoing compliance with regulatory requirements.

iGaming operators can effectively mitigate the risks associated with money laundering and maintain the integrity of their operations within a complex and constantly evolving regulatory environment.

4. Customer Knowledge (KYC)

Identity verification processes

Identity verification processes are fundamental to compliance with Anti-Money Laundering (AML) policies in the iGaming sector. These processes aim to ensure that customers are who they say they are and that their financial transactions are legitimate. Common KYC practices include:

Information Collection: Requesting personal information from customers, such as full name, address, date of birth, and identification number.

Supporting Documentation: Verification of valid identity documents, such as a passport, driver's license, or national identity card, to confirm the customer's identity.

Electronic Verification: Use of electronic identity verification services that validate personal information through reliable databases and public records.

These processes ensure that customers are effectively authenticated and their personal information is verified before allowing them to participate in online gaming activities. This not only helps prevent money laundering, but also protects against the use of fake or stolen identities.

Reliable sources of information

iGaming operators must use reliable sources of information. That includes:

Government Databases: Query identification records issued by government authorities, such as civil registries, tax records and national identification databases.

Verification Service Providers: Use of third-party verification services that have access to global and national databases to validate personal information, addresses and credit history.

Public Records: Access to public records that may provide information about criminal history, bankruptcies, or other relevant information about the client.

iGaming operators can improve the accuracy of identity checks and reduce the risk of fraud or illicit activity on their platforms.

Continuous monitoring of customers and transactions

Continuous monitoring of customers and transactions is essential to identify unusual patterns of activity that may indicate potential money laundering activities or other illicit practices. This process involves:

Transaction Analysis: Regularly monitoring customer financial transactions to identify suspicious activity, such as large volumes of deposits or non-typical withdrawals.

Behavior Analysis: Assessing customers' gambling behavior, including betting patterns, gambling frequency, and sudden changes in activity patterns.

Customer Profile Update: Periodically review customers' KYC information to ensure it remains accurate and up-to-date over time.

iGaming operators can quickly detect and respond to potential money laundering threats, thereby protecting the integrity of their operations and complying with AML regulatory requirements.

These KYC practices are critical to ensuring that iGaming operators operate within the highest standards of regulatory and ethical compliance, while protecting their customers against fraudulent and illegal activities.

5.Third Party Due Diligence

Due Third-Party Diligence is a critical process within an AML program, aimed at mitigating risks associated with money laundering and terrorist financing. This process involves detailed assessment of third parties, such as customers, suppliers and business partners, to ensure they are not involved in illicit activities. Includes verification of identity, financial history, business reputation, and compliance with relevant laws and regulations. The Due Third-Party Diligence not only protects the company against legal and reputational risks, but also strengthens the integrity of the business environment.

Assessment of Business Partners and Suppliers

Business Partner and Supplier Assessment is an essential component of an effective AML program. It aims to ensure that business partners and suppliers comply with AML policies and regulations. This assessment includes analysis of the company's reputation, financial due diligence, regulatory compliance, and ethical business practices. The company must establish clear criteria for continuous evaluation of partners, ensuring that they maintain adequate standards throughout the commercial relationship.

Contracts and Agreements that Include AML Clauses

Contracts and Agreements that Include AML Clauses are fundamental legal instruments to ensure compliance and mitigate risks related to illicit activities.

Such clauses impose obligations on contracting parties to report suspicious activity, perform due diligence on customers and transactions, and maintain accurate and accessible records for regulatory inspection. Including AML clauses in contracts strengthens a company's position by demonstrating a commitment to regulatory compliance and business integrity.

6. Transaction Monitoring and Control

Transaction Monitoring and Control

Transaction Monitoring and Control are crucial components of an effective AML (Anti-Money Laundering) program, designed to detect and mitigate illicit activities such as money laundering and terrorist financing. This process involves ongoing supervision of financial transactions and the application of preventive and corrective measures as necessary.

Tools and Technologies Used for Monitoring

To carry out Transaction Monitoring efficiently, financial institutions and other entities use a variety of Tools and Technologies. This includes automated anomaly detection systems, analysis of customer behavior patterns, artificial intelligence and machine learning to identify suspicious transactions. Additionally, data analysis software and risk management programs are employed to monitor and analyze large volumes of transactions in real time.

Warning Indicators for Suspicious Transactions

Warning Indicators are signals that may suggest the occurrence of suspicious transactions that require further investigation. Common examples include unusual transactions for the customer's profile, frequent deposit and withdrawal activities of large amounts of money, transfers to or from countries with a high risk of money laundering, and transaction patterns inconsistent with the customer's behavioral history. Identifying and analyzing these indicators are essential to mitigating risks and complying with AML regulations.

Procedures for Reporting Suspicious Transactions to Authorities

The Procedures for Reporting Suspicious Transactions are rigorous and fundamental to combating money laundering. Institutions must establish clear policies for identifying, documenting and reporting suspicious transactions to competent authorities. This generally involves collecting relevant evidence, completing specific reporting forms, and communicating promptly and confidentially with financial intelligence units or designated regulatory authorities. Following these procedures not only helps avoid legal and financial complication, but also strengthens the integrity of the global financial system. Transaction Monitoring and Control are fundamental pillars of an effective AML program, essential to protect financial institutions and other entities against criminal activity. By implementing advanced tools, identifying red flags and following clear

procedures for reporting suspicious transactions, organizations not only meet their regulatory responsibilities but also contribute to a safer and more transparent business environment.

7. AML Training and Awareness

AML Training Programs for Employees

AML Training Programs (Anti-Money Laundering) are critical to enabling employees to recognize and respond to suspicious activity that may indicate money laundering or terrorist financing. These educational programs should cover the basic principles of AML, internal company policies, due diligence procedures, diligence, identification of suspicious transactions and the importance of adequate reporting to the competent authorities. Training must be ongoing and adapted to the different levels and roles of employees, ensuring that everyone understands their responsibilities and contributes to the company's compliance and security.

Regular Updates on Regulations and Best Practices

Maintaining regular updates on AML regulations and best practices is essential to ensure that employees are always informed about changes in laws, new regulatory guidelines and developments in the anti-money laundering field. This may include workshops, seminars, internal newsletters, and educational materials that cover case studies, market trends, and lessons learned from money laundering investigations. Keeping employees up to date not only strengthens technical knowledge, but also reinforces the culture of compliance and ethics within the organization.

Investing in AML Training and Awareness is not only a regulatory obligation, but also a proactive strategy to protect the company against financial and reputational risks. By empowering employees with up-to-date knowledge and robust AML practices, organizations not only meet their legal responsibilities but also promote a safe, ethical and resilient work environment.

8. Audit and Internal Review

Internal Audit for Compliance with AML Policies

Internal auditing is a systematic and independent process to determine whether an organization's policies and procedures are being followed correctly. In the context of AML, this involves:

Audit Planning:

Identification of critical processes and areas related to AML that will be audited.

Definition of specific audit objectives, such as reviewing suspicious transactions, verifying the adequacy of internal controls, etc.

Audit Execution:

Gathering evidence through document review, interviews with key employees and data analysis.

Application of tests to verify the effectiveness of internal controls, such as reviewing transaction records, checking due customer due diligence, among others.

Analysis and Report:

Assessing audit findings against established AML policies.

Documentation of non-conformities and recommendations for improvements.

Preparation of reports for senior management and audit committee, highlighting areas of concern and corrective action plans.

Example: A financial services company conducts an internal audit focused on AML compliance. During the process, they randomly review 100 recent transactions, checking whether due diligence procedures diligence were applied correctly. They find that in 20% of cases there was no adequate documentation. This results in recommendations to improve customer verification procedures.

Periodic Reviews of Policies and Procedures

In addition to auditing, periodic reviews of policies and procedures are crucial to ensure they remain up to date and effective:

Assessment of Regulatory Changes:

Continuous monitoring of new regulations or changes to existing ones that may affect AML policies.

Adapting company policies to reflect these changes, ensuring ongoing compliance.

Feedback and Continuous Improvement:

Collecting feedback from employees involved in implementing AML policies.

Analysis of incidents or non-conformities to identify areas that require adjustments.

Example: A financial technology company reviews its AML policies annually. During this year's review, they identify new regulation that requires additional identity verification for international transactions. As a result, they update their customer verification procedures to include these new guidelines.

These internal audit and ongoing review processes are critical to ensuring that an organization is not only compliant with AML policies, but also proactively

prepared to deal with regulatory changes and new challenges in combating money laundering and terrorist financing.

9. Risk Management

Assessment and Mitigation of Specific Risks in the iGaming Sector

Risk Identification:

Fraud and Money Laundering: Due to the financial nature of transactions in iGaming, there are significant risks of fraud and money laundering. This may involve fraudulent transactions, manipulating game results, or using platforms to launder illicit money.

Cybersecurity: The industry faces constant cyber threats such as phishing attack, ransomware and data breaches. Protecting player data and transaction security is critical to reputation and regulatory compliance.

Regulatory Compliance: Different regions have varying regulations regarding online gambling. Failure to comply with these standards can result in severe fines, loss of licenses and damage to the company's reputation.

Risk analysis:

Use of methods such as vulnerability analysis, impact and probability assessment, and scenario modeling to identify and prioritize risks.

Risk Mitigation:

Internal Controls: Implementing robust controls to monitor transactions, detect suspicious behavior and ensure compliance with regulations.

Advanced Technology: Use of advanced cybersecurity solutions, such as firewalls, encryption and intrusion detection systems (IDS), to protect critical infrastructures and sensitive data.

Training and Awareness: Ongoing employee education on safe work practices, cyber threat recognition, and incident response procedures.

Strategies for Dealing with New Types of Threats

Proactive Monitoring:

Establishing real-time monitoring systems to identify unusual patterns of activity that may indicate new threats.

Collaboration and Information Sharing:

Participation in information sharing initiatives between companies in the sector for early warnings about new threats and best security practices.

Continuous Adaptation:

Regularly review and update security policies and procedures to incorporate new types of threats as they emerge.

Example: An iGaming operator implements a new artificial intelligence-based fraud detection system to analyze betting and transaction patterns in real time. During the testing phase, the system identifies a number of suspicious transactions that would not have been detected using traditional methods. This allows the company to adjust its internal controls and strengthen its defenses against new types of fraud.

Effective risk management in iGaming is not only crucial for security and compliance, but also for the sustainability and continued growth of operations in the increasingly complex and dynamic digital environment.

10.Documentation and Registration

Maintaining Adequate Records of AML Transactions and Procedures

Importance of Documentation:

iGaming operators are required by regulations to maintain detailed records of financial transactions, customer identity verification, and any suspicious activities related to money laundering and terrorist financing (AML/CFT).

Audit and Accountability: Accurate and complete documentation facilitates internal and external audits, demonstrating compliance with regulatory standards and good corporate governance practices.

Types of Documents to be Maintained:

Financial Transactions: Records of deposits, withdrawals, transfers and other financial transactions carried out by players.

Identity Verification: Documentation used to verify the identity of players, such as copies of identification documents, proof of residence, among others.

Suspicious Activity Reports (SARs): Documentation of any suspicious activities reported to appropriate authorities as required by AML regulations.

AML Procedures:

Due Customer Diligence : Records of due diligence procedures Due diligence applied to verify players' identity and source of funds as required by AML regulations.

Continuous Monitoring: Documentation of continuous transaction monitoring processes to detect suspicious activity and report as necessary.

Secure Storage and Confidentiality of Documents

Information security:

Using robust security technologies, such as data encryption, firewalls, and controlled access, to protect records from unauthorized access and data breaches.

Document Retention Policies:

Establishment of clear document retention policies to ensure that records are kept for as long as necessary and then properly disposed of, in accordance with regulatory and legal requirements.

Controlled Access and Audit:

Implementing access controls to ensure that only authorized personnel are allowed to access sensitive documents.

Carrying out regular audits to verify compliance with document security and confidentiality policies.

Example: An iGaming platform keeps detailed records of all players' financial transactions, including deposits, withdrawals and winnings. During an internal audit, it was discovered that some players' identity verification records were not being maintained properly. This resulted in a review of identity verification procedures and an increase in documentation required to ensure compliance with AML regulations.

Proper documentation and secure storage are essential pillars for transparent and legally compliant operation in the iGaming sector , ensuring not only regulatory compliance but also player trust and integrity of operations.

11.Examples and practical cases

Case Studies of Money Laundering Incidents in the iGaming Sector

Case Study 1: Manipulation of Game Results

iGaming operator is investigated on suspicion of money laundering related to the manipulation of game results. Players are consistently winning in high stakes gambling games, suggesting possible fraudulent coordination to launder illicit money through seemingly legitimate winnings.

Consequences: The investigation results in the loss of the operator's license and substantial fines for failing to implement adequate controls to detect and mitigate fraudulent activity.

Lessons Learned: Implement robust gaming monitoring systems to detect unusual winning and losing patterns, and regularly review AML compliance practices to prevent manipulation and fraud.

Case Study 2: Using Platforms for Illicit Transactions

Description: An iGaming platform is inadvertently used by criminals to launder money from illicit activities. Significant and frequent transactions are made without adequate verification of identity or source of funds, violating AML regulations.

Consequences: The company is the target of a regulatory investigation that reveals flaws in due diligence procedures customer due diligence and monitoring suspicious transactions. This results in financial penalties and mandatory reviews of compliance protocols.

Lessons Learned: Strengthen identity verification controls and implement automated monitoring systems to detect and report suspicious transactions as required by AML regulations.

Examples of Best Practices and Common Mistakes to Avoid

Best Practices:

Due Strict Customer Diligence : Full verification of players' identity, including valid documentation and source of funds checks.

Continuous Transaction Monitoring: Implementation of automated systems to detect suspicious transaction patterns and unusual activities.

Ongoing Employee Training: Regular education on AML/CFT regulations and compliance practices for all employees involved in gaming and betting processes.

Common Mistakes to Avoid:

Lack of Adequate Internal Controls: Failure to implement robust controls to detect and mitigate suspected money laundering activities.

Ignoring Suspicious Activity: Failing to report potentially fraudulent activity or carrying out adequate investigations when red flags are identified.

Lack of Compliance with Local and International Regulations: Not properly following AML/CFT regulations specific to iGaming operations in different jurisdictions.

Best Practice Example: An iGaming operator implements a new identity verification system that includes two-step verification for all new player registrations. This helps significantly reduce the number of fraudulent accounts and increases compliance with AML regulations.

Example of a Mistake to Avoid: An iGaming platform receives repeated reports of suspicious transactions on a specific account but does not adequately investigate or report these activities to the appropriate authorities. This results in a regulatory investigation that reveals a lack of due diligence in AML compliance and results in severe penalties.

iGaming operators strengthen their AML/CFT compliance protocols, protect against illicit activity, and maintain the long-term integrity of their operations.

12. Attachments

a) Glossary of terms related to AML

The glossary of terms related to AML (Anti-Money Laundering), it is important to include detailed definitions and practical examples for better understanding. Here are some terms with their definitions and examples:

Know Your Customer Your Customer - KYC):

Definition: Process used by financial institutions to verify the identity and financial history of their customers.

Example: A bank carries out checks on a customer's identity, address and source of funds before opening a bank account.

Suspicious Transaction:

Definition: Any financial transaction that appears unusual or inconsistent with the customer's pattern of activity.

Example: A series of fair cash deposits below the threshold for mandatory reporting may indicate an attempt to avoid detection.

Exchange of Financial Information (Financial Action Task Force - FATF):

Definition: Intergovernmental organization that develops policies to combat money laundering and terrorist financing globally.

Example: The FATF issues guidelines that member countries must follow to strengthen their AML/CFT systems.

Politically Exposed (Politically Exposed Person - PEP):

Definition: Individuals who hold or have held significant political positions or important roles in international organizations.

Example: A high-level manager of a foreign state-owned company may be considered a PEP due to his political influence.

Money laundry:

Definition: The process of disguising the origin of illegally obtained funds by making them appear legitimate.

Example: A criminal who uses a complex network of transactions to hide the source of money obtained through criminal activities, such as drug trafficking.

Statement of Suspicion:

Definition: Report that a financial institution must submit to regulatory authorities when identifying suspicious activity.

Example: A bank employee observes unusual transaction patterns on an account and files a suspicious statement with the financial regulator.

Due Due Diligence :

Definition: Process of investigation and analysis before entering into a business or financial relationship to mitigate legal and compliance risks.

Example: Before offering banking services to a new customer, the bank conducts a due diligence diligence to assess the risk of money laundering.

b) Regulatory and legislative references

Regulatory Body:

iGaming activities , including AML measures.

Example: Malta Gaming Authority (MGA) regulates iGaming operators in compliance with AML guidelines.

Fourth Anti-Money Laundering Directive (AMLD4):

Definition: European Union directive that establishes standards to prevent the use of the financial system for money laundering and terrorist financing.

Example: AMLD4 requires iGaming operators to implement robust KYC procedures and report suspicious transactions.

Fifth Anti-Money Laundering Directive (AMLD5):

Definition: Update to AMLD4 that expands the scope of AML obligations to include cryptocurrency platforms and strengthens due diligence requirements.

Example: AMLD5 imposes more stringent requirements for the identification of final beneficiaries and cooperation between national authorities.

Financial Intelligence Unit (FIU):

Definition: Authority responsible for receiving, analyzing and disseminating information about suspicious transactions to combat money laundering.

Example: The Gibraltar FIU receives reports from iGaming operators about suspicious activity and forwards them for investigation.

Malta Bank Secrecy Law:

Definition: Legislation regulating the confidentiality of financial information in Malta, adapted to include iGaming operators .

Example: The law imposes restrictions on sharing information about customers, except in cases of AML investigations conducted by competent authorities.

Payment Services Directive (PSD2):

Definition: EU directive that regulates payment services and introduces new security and authentication requirements for online transactions.

Example: PSD2 affects iGaming operators offering payment services, requiring strong customer authentication and anti-fraud measures .

c) KYC form templates

Model 1: KYC Form for Individuals

Personal information:

Full name:

Date of birth:

Nationality:

Identification document number (passport, ID, etc.):

Full residential address:

Contact Details:

Phone number:

Email address:

Employment Information:

Employer name:

Office:

Sources of Funds:

Origin and nature of the funds to be used in the commercial relationship.

Other information:

PEP Declaration (Politically Exposed Person), if applicable.

Model 2: KYC Form for Legal Entities

Company Information:

Corporate reason:

Date of establishment:

Registered address:

Final Beneficiary Details:

Full name of the final beneficiary:

Participation percentage:

Authorized Representative Details:

Full name of authorized representative:

Office:

Necessary documents:

Copy of company registration.

Identification documents of the final beneficiary and authorized representative.

Template 3: KYC Update Form

Updated Data:

Report any significant changes to the information previously provided.

Reason for Update:

Justify the need to update the information.

Supporting Documentation:

Include documents supporting the changes reported, if applicable.

Template 4: Declaration of Origin of Funds

Source of Funds:

Detail the source of funds to be used in the transaction.

Nature of the Transaction:

Describe the purpose of the transaction and its relationship to the account or service requested.

Certification:

Customer signature confirming the veracity of the information provided.

Template 5: Suspicious Transaction Report Form

Suspicious Transaction Details:

Description of the suspicious transaction, including value, date and those involved.

Reason for Suspicion:

Explain why the transaction is considered suspicious.

Evidence and Documentation:

Include any documents or evidence that supports the suspicion raised.

***These templates can be adjusted as needed to meet specific company requirements and local AML regulations. It is important to review and update these forms regularly to ensure they are aligned with current best practices and standards.