

AML/CTF Policy (Miranda Path B.V.)

Version 1

Abstract:

This document defines Miranda Path B.V. Anti-Money Laundering policy. All employees and processes within will be set up to ensure compliance to this policy.

Confidentiality notice.

This document contains proprietary information and is for internal use only. It may not be shared or disclosed without permission.

All rights are reserved. This document may not, as a whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent, in writing, from an authorized representative of Miranda Path B.V.

Document Synopsis

This document defines Miranda Paths Anti-Money Laundering policy. All employees and processes within will be setup to ensure compliance to this policy.

Documentation Control

Version 1.0	Date 08/12/2025	Reason for Issue – Policy creation	Issued By
--------------------	------------------------	---	------------------

Documentation Approval

Name	Role	Date	Signature
Hayley Beecroft	Chief Commercial officer	08/12/2025	

Table of Contents

ANTI-MONEY LAUNDERING POLICY	4
ANTI-MONEY-LAUNDERING POLICY	4
INTRODUCTION	4
SANCTIONS POLICY	4
PARTICIPANTS	6
REGISTERED CUSTOMERS (RC) AND SUPER MASTER AGENT (SMA) ACCOUNTS	6
REGISTRATION OF MASTER AGENTS (MA)	7
KYC FOR SMAS, MASTER AGENTS AND AGENTS	8
CUSTOMER DUE DILIGENCE MEASURES	9
ENHANCED DUE DILIGENCE	10
EXAMINATION OF TRANSACTIONS	10
DEPOSITS/PAYMENTS OF WINNINGS	11
ACCEPTANCE OF WAGER	11
ACCOUNT CLOSURE	11
FINANCIAL TRANSACTION – RECORD & REPORT	11
IDENTIFICATION AND VERIFICATION OF IDENTIFY	12
DEPOSITS, WITHDRAWALS	12
RETENTION OF RECORDS	12
REPORTING OF SUSPICIOUS TRANSACTIONS	13
RECORD KEEPING	20
BUSINESS ASSOCIATES, FOREIGN BRANCHES AND SUBSIDIARIES (GENERAL)	22
RISK ASSESSMENT	24

ANTI-MONEY LAUNDERING POLICY

1.) Policy Approval

Introduction: Miranda Path B.V. (The “Company” is a company registered and incorporated in Curacao under company Registration number **162727**

The Company is committed to ensuring that it takes all appropriate steps to prevent its systems from being used for the purposes of Money Laundering, Terrorist Financing or other associated Crimes. These Steps Include But are not Limited to;

- The appointment of a Suitably qualified Anti-Money Laundering & Compliance officer
- Board Approved policies and procedures
- Risk-Based Approach to all business relationships
- Applying appropriate use of technology and tools to help identify and mitigate risk
- Ensuring all employees are suitably trained
- Reporting Suspicious activity to the relevant law enforcement agencies
- An Annual Independent audit of Miranda Path’s Anti-Money Laundering compliance program.

This Document has been produced to ensure that the company (Miranda Path B.V.) acknowledges and applies appropriate measures to address the higher level of risks associated with the Business and its day-to-day operations.

This Document has been reviewed and approved by the resolution of the management board of the company.

All future versions and updates will be reviewed by the management board before being approved and issued.

All changes, Additions and approvals to this policy will be accurately recorded on “**Page 2**” for record and document control purposes.

2.) General Provisions

The company is in the process of obtaining a license with the CGA (Curacao Gaming authority) to offer interactive (Online) Remote betting and gambling products (Game of Chance) and services under Supplier License xxxxx issued by the Curacao Gaming Control Board (GCB)

Gaming License Application Number: QPA/2025/04178

In accordance with the National Ordinance on Games of Chance (Landsverordening op Kansspelen) “LOK”)

Under the terms of its operating license the company is required to have in place adequate policies, processes and procedures to prevent its systems from being used for the purposes of money laundering, proliferation financing, terrorist financing or other criminal activity.

This document will be reviewed on both a regular basis and ad-hoc basis as required by changes to laws and regulations, changes to license conditions, Introduction or implementation of new products and services or in accordance with the company’s risk management practices and procedures.

3.) Laws & Regulations

The designated supervisory Authority for service providers offering services from the jurisdiction of Curacao, or under a license issued by the (Curacao Gaming Authority)

<u>Applicable Laws</u>
➤ The National Ordinance Criminal Code (P.B. 2011, no 49);
➤ The National Ordinance of November 23, 2015 amending the National Ordinance identification for services (P.B. 2015, no. 69);
➤ The National Ordinance on Identification when Rendering Services or NOIRS
➤ (Landsverordening identificatie bij dienstverlening (LID), PB 2017, no. 92); and
➤ The National Ordinance on the Reporting of Unusual Transactions or NORUT
➤ The National Ordinance on the Reporting of Unusual Transactions or NORUT
➤ (Landsverordening melding ongebruikelijke transacties (LMOT), PB 2017, no. 99).
➤ Sanctions National Ordinance
➤ Kingdom Sanction Act
➤ Ministerial Decree on Indicators of Unusual Transactions
➤ National Decree – Kingdom Sanction Law Enactment

4.) Definitions

Money Laundering

Money Laundering is defined as.

- the conversion or transfer of funds or property derived from criminal activity.
- retaining funds or property derived from criminal activity.
- participation in such activity such as for the purposes of concealing, or disguising the illicit origin
- of the funds or property or assisting any person who is involved in the commission of such an
- activity to evade the legal consequences of that person's actions
- acquisition, possession or use of funds or property derived from criminal activity, or property
- obtained instead of such funds or property, knowing, at the time of receipt, that such funds or
- property was derived from criminal activity or from an act of participation
- the concealment or disguise of the true nature, source, location, disposition, movement, rights
- with respect to, or ownership of, funds or property derived from criminal activity.

Furthermore, Money Laundering Consists of three Phases:

- **Placement** - During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, casinos, shops and other cash intensive businesses. This is done among other things by buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requests for pay out and inserting funds into gaming machines and immediately claiming those funds as credits.
- **Layering**. This stage involves converting the proceeds of crime into another form to disguise the audit trail, source and ownership of funds. It can involve transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing money and hiding them from the authorities.
- **Integration**. The re-entry of funds into the economy in what appears to be normal business or personal transactions. Examples are the purchase of luxury assets, financial investments, investing in gaming companies or commercial investments

Terrorist Financing

Terrorist financing is defined as.

- The allocation or raising of funds to plan or perform acts which are deemed to be acts of terrorism or to finance operations of terrorist organizations, or in the knowledge that the funds allocated or raised will be used for the aforementioned purposes.

The most basic difference between financing of terrorism and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit process. Money laundering always involves the process of illegal activity. There is a need for the terrorist group to disguise the link between it and its legitimate funding sources, in doing so the terrorists use methods similar to those criminal organizations use to launder money like smuggling, structuring, wire transfers, purchase of monetary instruments, use of debit and credit cards. While ML is concerned with obscuring the source of funds, FT is most concerned with obscuring the end receipt of the funds.

Proliferation Financing

In October 2020, the Financial Action Task Force revised its standards (R1 and INR 1) to require Countries, Financial Institutions and designated non-financial businesses and professions to identify, assess, understand and mitigate their Proliferation Financing risks.

Proliferation financing ("PF") refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual- use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligation.

According to FATF, PF Risk Indicators include those relating to;

- Customer profile
- Account and transaction History
- Maritime sector Risk indicators
- Trade Finance

Further guidance on PF risk indicators, issued by FATF, can be found at [Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf \(fatf-gafi.org\)](https://www.fatf-gafi.org/publications/guidance/Proliferation-Financing-Risk-Assessment-Mitigation.pdf)

Staff should familiarise themselves with the typologies and red flag indicators of PF as documented by FATF, in order to identify circumstances in which customers and transactions may present PF risks. Any risks identified will be mitigated by such measures as.

- A. Sanctions screening to identify any potential sanctions evasion
- B. Enhanced customer due diligence procedures.
- C. Effective maintenance of customer master data.
- D. Ongoing compliance monitoring

High Risk Country

A high-risk country is defined as:

A country or territory where the risk of money laundering, terrorism or financial or other crime is considered to be higher than other countries or territories. as may be determined by organizations such as:

- European Union
- United Nations
- Financial Action Task Force (FATF)
- Moneyval
- International Monetary Fund (IMF)
- US Office of Foreign Asset Control (OFAC)

The term high risk can be applied to either the country or jurisdiction or to nationals, citizens or residents of the country or jurisdiction. Equally, Nationals, Citizens, or residents of high-risk countries or Jurisdictions may be subject to sanctions checks preventing or limiting a business relationship.

Politically Exposed Person (PEP)

A politically exposed person is defined by the National ordinance on identification when rendering services (NOIRS) as:

- An individual or person who holds has a prominent public function with the exception of those who have held this position for less than a year, and the immediate family members or close associates of these persons.

Sanctions

Sanctions may be imposed on countries, companies or individuals.

Sanctions listed individuals are defined as:

- Individuals subject to regulatory or financial sanctions or enforcements, known terrorists, money launderers, fraudsters and black-listed persons.

Targeted financial sanctions require countries to freeze funds and assets and to ensure that no funds and other assets are made available, directly, or indirectly, to or for the benefit of any designated persons or entities.

5.) Risk Based Approach

The Company is committed to taking a risk-based approach through its Anti-Money Laundering Compliance Program. Its primary goal is to protect the organization against money laundering and to ensure that the organization is in full compliance with relevant laws and regulations.

The company will implement a set of policies and practices to identify and mitigate risks including:

- identify and assess the level of risk (low to high)
- assess the impact of risks identified
- identify and implement controls to mitigate against the risk and its impact
- ensure on-going monitoring to evaluate and ensure the effectiveness of the controls
- periodically review and update its risk management policies and processes in accordance with events, the introduction of new products or technology or changes in laws and regulations.

The company will conduct a full assessment in relation to identifying and implementing controls to mitigate:

Business Risk Assessment (BRA)

The compliance officer will perform a review of all of the ML/FT/PF risks that the business faces and document such risks in the Business Risk Assessment. The Business Risk Assessment will record the identified risks, the assessment of these risks and the controls and mitigations in place to prevent such risks from materialising

In identifying and assessing risk, consideration will be given to factors such as;

- Regulatory environment and potential changes
- National Risk Assessments relating to Curaçao
- The type of business undertaken by the client
- Product/service offered to the client

The risk assessment will include the following:

- A description of the risk
- The probability of the risk occurring and the impact it will have on the Company (Miranda Path B.V.)
- A description of the mitigations and controls in place to reduce the risk

The Business risk Assessment will be reviewed at least annually and when circumstances change or new threats emerge.

In order to identify emerging risks for inclusion in the Business Risk Assessment, the Compliance Officer will compile an annual compliance report which will include findings from review of relevant law enforcement alerts and reports, thematic reviews issued by the relevant regulatory bodies in Curaçao and industry specific risk guidance.

Customer Risk Assessment (CRA)

The Company is required to have and follow reasonable procedures to document and verify the identity of customers prior to establishing a business relationship with them.

All customers are to undergo a full risk assessment prior to being onboarded as a client. Customers are categorized as either low, standard or high risk. Below is the criteria for each risk rating.

High Risk:

- The business relationship is conducted in unusual circumstances
- The customer is a resident or transacts with a geographical area of high risk
- The corporate structure of the customer is unusual or excessively complex given the nature of the company's business
- Politically exposed person (PEP)

Where a customer is deemed to be high risk, they will undergo enhanced due diligence (EDD) checks with additional ongoing monitoring.

Low Risk:

- Any company whose securities are listed on a regulated market will be considered as low risk.

A Low -Risk client will undergo standard CDD checks and ongoing monitoring.

Standard Risk Customer

- Any customer who does not have any high- or low-risk factors will be classified as standard risk.

This category will undergo standard CDD checks and ongoing monitoring to assess any changes which may lead to the client being recategorized as high risk.

Technology Risk Assessment (TRA), Product Risk Assessment (PRA)

The Company will undertake a risk assessment of any new technology it intends to use in the business or any products it intends to distribute. The potential risks will be considered under the following categories.

- Operational risks: Losses that may arise due to deficiencies in system reliability or integrity. This will also take into account how the product interacts with customers and the methods in which payments for the product are received.
- Reputational risks: Negative public reactions caused by system or product failure
- Legal risks: Failures resulting in violations or non-compliance with legislation.

An assessment will be performed for each new technology and will cover risk identification, vulnerability, consequence and mitigation.

A log of all risk assessments undertaken will be maintained by the Compliance officer and will be presented to the board annually. All risk assessments will be documented appropriately detailing the measures undertaken and the reason for the assessment.

6.) Customer Due Diligence

The Company will apply appropriate customer due diligence measures to all customers in accordance with applicable laws and regulations. As Miranda Path operates on a B2B basis, providing software services to licensed Operators & Aggregators rather than directly to players, due diligence will focus on the identification and verification of these B2B customers. Where relevant, initial due diligence will also include checks relating to technical identifiers due to the digital and virtual nature of the services provided.

The Company shall use a risk-based approach when undertaking ongoing customer due diligence, in accordance with this policy and the customer risk assessment.

The Company shall perform CDD prior to establishing business relationships. New customers will be asked to complete an onboarding form and provide CDD documents as per the below, as supporting evidence.

Statutory Documents – Company

Documents must be certified by a current acting director of the company

- Company statutory documents
- Individual CDD for all Directors, beneficial owners who own more than 10% of the business and any other applicable authorised individuals (please see above for Proof of Address and Proof of Identity Documentation and certification requirements for individuals)
- Corporate Structure
- Bank statement must be in the name of the business registering and dated within 6 months and certified.

Proof of Identity – Individual Basis.

Documents must be certified by a lawyer, notary, member of an accredited body, Certified chartered accountant or other public recognised official.

Below is a list of the following acceptable forms of Proof of Identity (ID)

- **Passport** - This must be in date, a colour copy, and show both the photographic page and the opposing page clearly including all edges.
- **Driving License** - We require only the front of the driving licence. This must be in date. If a driving licence is used as ID it cannot be used for Proof of Address.
- **National Identity Card** - Both sides of the Card is required. The card must be in date.

Proof of address (POA)

Documents must be certified by a lawyer, notary, member of an accredited body, Certified chartered accountant or other public recognised official.

- **Utility Bill**
- **Driving License** (This cannot be used as ID if used here)
- **Bank Statement** (This should be a personal bank statement, in the name of the individual)

PEP's (Politically exposed persons) & Sanctions:

The definition of a Politically Exposed Person (PEP) in the National Ordinance on Identification when Rendering Services (NOIRS) is as follows.

Persons who hold or have a prominent public function with the exception of those who have held this position for less than a year, and the immediate family members or close associates of these persons.

In line with its obligations (Article 2 of NOIRS), the Company will:

- Implement appropriate risk management systems to determine whether a client or ultimately interested party is politically vulnerable.
- obtain approval from the persons responsible for the overall management of the service provider, for entering into a business relationship with or effecting a transaction for such client, or beneficial owner as well as obtaining such approval if during the business relationship the client or beneficial owner becomes a politically exposed person;
- take risk-based and adequate measures to identify the source of political capacity prominent person and the funds used in the business relationship or transaction to pose; and
- maintain on-going monitoring and tight control of the business relationship

The following persons shall be persons performing prominent public functions, and subject to a PEP check:

- a state, head of government, minister and deputy or assistant minister
- A member of parliament or of a similar legislative body, a member of a governing body of a political party, a member of a supreme court, a member of a court of auditors, or of the board of a central bank.
- An ambassador, or a high-ranking officer in Armed forces
- A member of an administrative, management or supervisory body of a state-owned enterprise
- a director, deputy director or member of the board, or equivalent function, of an international organization, except middle-ranking or more junior officials.
- the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person or a local politically exposed person.
- a parent of a politically exposed person or local politically exposed person

The following persons are considered close associates of a person performing prominent public functions:

- a natural person who is known to be the beneficial owner or to have joint beneficial ownership of a legal person or a legal arrangement, or any other close business relations, with a politically exposed person or a local politically exposed person;
- a natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person or local politically exposed person.

Where a PEP is positively identified, the Company will conduct a full review and gain approval from the management board or service provider prior to establishing a business relationship.

The Company will conduct on-going PEP screening checks as part of its on-going due diligence procedures.

- the type of public function of the PEP.
- the country from which the PEP originates.
- the transactions that the PEP carries out.

Enhanced Due Diligence

The Company shall conduct Enhanced Due Diligence procedures when a customer has been identified as high risk. Customers should be continually monitored by the Company for any update in their risk profile. Where behaviors or transactions are identified which may increase the Customer's potential risk, further investigations and due diligence should be undertaken. Factors which may increase a customer's risk include suspicious activity, a match against a PEP/Sanctions list or a sudden change in behavior, for example conducting transactions that are not in line with the customer's business objectives.

EDD measures include, but are not limited to, the following measures:

- Obtaining an additional method of photo ID
- Obtaining proof of source of funds / wealth (Acceptable documents listed below)
- Verifying disclosed information through public sources, companies' registry etc.

Source of wealth Documents acceptable

- Payslips
- Letter from employer confirming annual salary
- Latest Audited accounts and company bank statement

Sale of property

- Signed letter from a solicitor
- Certified copy of sales contract
- Signed letter from recognized estate agent

Inheritance

- Signed letter from solicitor
- Probate with a copy of the will

Termination of a business relationship

In the cases where the above due diligence onboarding requirements of this document cannot be met, the company shall not establish the business relationship with the customer. In those cases where the business relationship is already established, however there is reasonable ground to for suspicion of any ML/FT/PF activity, the company might also terminate the business relationship with the customer. This action would be followed by an appropriate report to the FIU. Termination of the business relationship might also occur in those scenarios where the customer is reluctant to provide sufficient documentation to verify their identity.

In all the scenarios the company will document all the factors and information it has in it its disposal as well as the steps taken in order to make the necessary documentation and information available.

Ongoing Monitoring:

The Company (Miranda Path B.V.) has a continuing duty to conduct ongoing monitoring of all customer relationships and to be vigilant with regard to money laundering and terrorist financing at all times and to report any suspicious transactions or circumstances.

The Company (Miranda Path B.V.) will monitor all customer transactions and activity in accordance with the industry's best practice, international recommendations and guidelines.

The Conditions of ongoing monitoring such as frequency or the extent of the checks shall be determined by the risk level assigned during the stage of risk assessing the customer.

Miranda Path B.V. will review any client who is classified as high risk every twelve months, all medium – and low risk clients will be reviewed every two years. The review ensures all due diligence information is still relevant and up to date. This includes:

- Checking identification and address is still valid; if not, this will be updated
- Checking there are no discrepancies on the person of significant control register
- Checking annual turnover is in line with what we would expect.

- A change in the client's identity
- A change in beneficial ownership of the corporate structure / client
- A change in the service provided to the client
- Information that is inconsistent with the business's knowledge of the client

7.) Reporting suspicious and unusual transactions

The Company shall submit a formal suspicious activity report to law enforcement in respect of any individual that is positively identified as being on a Sanctions list, in accordance with the process set out in the Company's AML Policy.

In accordance with Article 1 of the National Ordinance on the Reporting of Unusual Transactions or NORUT (Landsverordening meldingongebruikelijke transacties (LMOT), PB 2017, no. 99) ('NORUT') the Company has a duty to report unusual (suspicious) transactions which may be linked to money laundering, the financing of terrorism or other criminal activity. This duty is also stated in Article 4 of the AML/CFT/CFP - Regulations released on May 20, 2024 by the Curacao Gaming Control Board.

The company is required to Review & report not only suspicious transactions, but also unusual transactions. This is achieved by having adequate procedures in place where the following areas are being covered:

- The recognition of unusual transactions
- The Documentation of unusual transactions
- The reporting of unusual transactions

Where there are any concerns regarding any customer or any actual or attempted transaction, employees should in the first instance send an internal report to the Compliance Officer / Money Laundering Reporting Officer. The steps to making a formal report are as follows:

- An internal suspicious transaction report must be made to the Compliance Officer / Money Laundering Reporting Officer no later than 24 hours between the execution of the transaction (or the intention to execute a transaction).
- The Compliance Officer / Money Laundering Reporting Officer will have 10 working days to complete any additional investigations needed to ascertain the risk of money laundering, terrorist financing or other crime.
- Following the period of investigation any unusual (suspicious) transaction report must be submitted within 48 hours of the Money Laundering Reporting Officer making the decision to submit a report.

If this is not possible the Company will submit a request for dispensation (5 days) in writing to the FIU, stating the reasons for the extension.

The Money Laundering Reporting Officer will also notify the management board and/or service provider that a formal report has been submitted.

Submitting a formal unusual (Suspicious) Transaction report

All reports must be submitted using the FIU online reporting system: FIU Curaçao and goAML reporting portal. All supporting documentation is to be included in such report and available in English.

The Company and its senior management and employees shall not disclose any details or information in connection with a report filed to the FIU or a request for information made by the FIU. It is also not permitted to disclose information to the customer nor to third parties.

There are two types of indicators which are used to determine the type of report to be made:

- Objective Indicator – The circumstances under which a transaction is to be considered as Unusual.
- Subjective indicator - the transaction is considered unusual if the reporting entity (based on its knowledge of its clients, their income and their business activities, and any other circumstance that may be relevant) has reasonable indications to presume that a transaction is related to money laundering or terrorism financing. For subjective indicators, red flags can be suggested by the supervisors and/or the FIU that indicate such possible presumptions.

8.) Record Keeping

The Compliance Officer / Money Laundering Reporting Officer will maintain a full record and notify the management board and/or the service provider of the following:

- all internal reports received.
- review and decision-making process.
- all formal unusual (suspicious) transaction reports made to the FIU
- all individuals that are identified as a PEP
- all individuals that are identified as a possible Sanctions listed individual and the outcome of any review of that individual

The Company shall store and maintain for a period of minimum 5 years all necessary records on transactions. All records obtained through Due Diligence measures (such as ID cards, driving licenses, passports, and more) shall be also kept for a minimum period of 5 years since the date of the last occasional transaction or since the day due to which the business relationship with the customer has ended.

- **Anti-Money Laundering Program**

Introduction

An Anti-money laundering program is an essential component of the company compliance regime. The Primary goal of the program is to protect the organization against money laundering and to ensure that the organization is in full compliance with relevant laws and regulations.

The core elements the Anti-Money Laundering Compliance program is addressing are:

- A system of internal policies, procedures and controls
- A designated compliance officer with day-to-day oversight over the AML program
- An employee screening program and ongoing employee training program
- An independent audit function to test the AML program.

Miranda Path tests the anti-money laundering program systematically and adapts the program to the current risks that arise within the company's own organization. The AML program has the approval of senior management.

The Appointment of a Compliance Officer

The Company shall formally designate 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. The Company will also ensure that the designated individual has sufficient experience, time and resources in order to perform this role and its responsibilities.

The Duties of the Compliance Officer are, but not limited to:

- To design, implement and maintain 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 Company'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.

The current Compliance Officer is Angeline Hassan.

Name: Angeline Chen Hassan

Angeline@casterbridgepartners.com

Name	Role	Contact details	Date of Appointment
Angeline Chen Hassan	Compliance officer	Angeline@Casterbridgepartners.com	09/12/2025

9.) Restricted Jurisdictions

- Curaçao
- Netherlands
- France
- Spain
- Belgium
- Germany
- Lithuania
- USA
- UK
- Australia
- Estonia
- Afghanistan
- North Korea
- Iran
- Syria
- Yemen
- Serbia
- Myanmar
- Ukraine
- Portugal
- Russia
- Any other prohibited jurisdiction, jurisdiction on sanction lists, jurisdictions that deems online gambling illegal or blacklisted according to market and regulatory developments

