Know Your Customer (KYC) Policy

bridgepointsolutionsltd.com
Operated by: Bridgepoint Solutions Ltd
License No.:
Effective Date: 26.09.2025
Contact: yhesma@bridgepointsolutionsltd.com

1. Purpose of the Policy

The Know Your Customer (KYC) Policy sets out the procedures implemented by bridgepointsolutionsltd.com to ensure compliance with anti-money laundering (AML), counter- terrorist financing (CTF), and sanction screening regulations. These procedures are designed to protect the platform from being used for illicit purposes and to ensure that only verified, eligible individuals access its services. The policy supports regulatory obligations under Anjouan law and promotes transparency, trust, and responsible operation of the platform.

2. Scope and Legal Framework

This policy applies to all customers using bridgepointsolutionsltd.com, including those accessing services through affiliated domains or mobile applications. It also governs the activities of staff involved in customer verification, payments, risk assessment, and fraud detection. Additionally, it regulates interaction with high-risk geographies, Politically Exposed Persons (PEP) and suspicious transactions. The legal framework is based on the Anjouan Money Laundering (Prevention) Act 008 of 2005 and aligns with international best practices such as those defined by the Financial Action Task Force (FATF), and EU AML directives. The company is also subject to the General Data Protection Regulation (GDPR) where applicable.

3. Company Overview

Bridgepoint Solutions Ltd is a company incorporated under the laws of the Cyprus with registration number C224634. Its registered address is: Level 7/8 Tower C, 1 Exchange Square Wall Street, Ebene 1721-04, MU. The company operates bridgepointsolutionsltd.com under gaming license , issued by the Government of Anjouan, Union of Comoros, which authorizes it to conduct online gaming and wagering services in permitted jurisdictions.

4. Objectives

The policy aims to verify the identity of all users, prevent underage and unauthorized access, mitigate risks related to money laundering and financial crime, and ensure secure handling of personal data. It further aims to foster responsible gambling and adherence to licensing obligations. bridgepointsolutionsltd.com is committed to applying risk-based methods to prioritize attention and resources to higher-risk customers.

5. Customer Identification and Verification

Before being allowed to deposit over EUR 2,000 in total or request a withdrawal, a customer must complete a mandatory identity verification process. This process includes the collection of the customer's full legal name, date of birth, nationality, residential address, email address, and telephone number.

Customers must submit a valid, government-issued photo ID, such as a passport, national identity card, or driver's license. The document must clearly show the individual's

name, photograph, and date of birth. Additionally, customers must provide a recent utility bill, bank statement, or official correspondence, not older than three months, to verify the stated residential address.

6. Verification of Payment Ownership

bridgepointsolutionsltd.com requires proof that the payment method used to deposit or withdraw funds belongs to the customer. Accepted proof includes a bank statement, a screenshot of the customer's online banking dashboard, or an e-wallet interface showing both the method and the customer's name. Credit and debit cards must be personal and not corporate or third-party owned.

7. Enhanced Due Diligence (EDD)

In cases where the customer poses a higher-than-normal risk, such as politically exposed persons (PEPs), individuals from high-risk jurisdictions, or users engaging in unusual transaction behavior, or transactions exceeding $10,000 USD or groups of linked transactions exceeding $10,000 USD, enhanced due diligence will be performed. This includes requesting additional documentation, verifying the source of funds and wealth, conducting deeper database checks, more frequent monitoring of transactions, and requiring managerial approval to continue the relationship.

8. Risk Assessment and Categorization

bridgepointsolutionsltd.com classifies customers as low, medium, or high risk based on jurisdiction, deposit amounts, behavior, payment methods, use of anonymization tools (e.g. VPN), player type (PEPs or individuals with adverse media mentions) and other red flags. Risk categorization determines the extent of monitoring and frequency of updates required. High- risk users are subject to more detailed and frequent reviews, while low-risk users undergo standard verification and monitoring.

9. Continuous Monitoring

bridgepointsolutionsltd.com continuously monitors all user activity and financial transactions. The system is configured to detect unusual activity, including rapid deposits and withdrawals, high- risk geographies, use of proxy connections, and switching between multiple payment methods. Any unusual or suspicious behavior is escalated to the compliance team for review. Temporary restrictions may be applied until the review is completed.

10. Handling of Politically Exposed Persons (PEPs)

Politically exposed persons, their relatives, and close associates are flagged during onboarding and periodically rescreened during the customer relationship. bridgepointsolutionsltd.com uses third-party data sources to identify PEPs. Business relationships with PEPs require prior approval by the AML Officer or executive management and are subject to intensified monitoring.

11. Record Keeping and Data Protection

All documents collected during the KYC process, including ID scans, address proof, payment verifications, and internal communications, are securely stored for at least five (5) years following the end of the customer relationship. bridgepointsolutionsltd.com complies with GDPR and The Personal Information Protection and Electronic Documents Act (PIPEDA), Lei Geral de Proteção de Dados (LGPD), Australian Privacy Act 1988 and other relevant data protection

regulations. and ensures that personal data is stored securely, encrypted, and only accessible by authorized staff.

12. Reporting Suspicious Activities

All employees involved in customer interaction and payments are trained to detect and report suspicious behavior. Any such case must be reported internally to the AML Officer, who is responsible for determining whether to file a Suspicious Activity Report (SAR) with the relevant authorities. SARs must be filed within seven (7) days of identifying a suspicious transaction or behavior. Additionally, all transactions over EUR 10,000 or group of linked transactions that exeeding 10,000$ must be reported, regardless of whether they are deemed suspicious.

13. Employee Training and Compliance

bridgepointsolutionsltd.com provides regular training to all staff involved in compliance, finance, customer service, and fraud prevention. Training covers AML/CTF regulations, KYC best practices, fraud detection techniques, and data protection obligations. Records of training sessions, attendance, and certifications are maintained for internal audit purposes.

14. Internal audits

bridgepointsolutionsltd.com conduct internal audits to evaluate the effectiveness of KYC measures periodic on a basis.

15. Non-Compliance and Sanctions

Any customer who fails to complete KYC procedures will be restricted from transacting or accessing services on bridgepointsolutionsltd.com. Employees who violate this policy may face disciplinary action, including termination. The company may also face fines, license revocation, or criminal investigation in case of serious breaches. All customers and staff are required to cooperate fully with the compliance team.

16. Continuous Improvement

bridgepointsolutionsltd.com monitors and promptly updates KYC policies to align with changes in AML/CTF regulations. Additionally, it adopts advanced technologies, such as AI and blockchain, to enhance verification processes and maximize the reduction of fraud.

17. Contact Information

Support: yhesma@bridgepointsolutionsltd.com