



Breckenridge Curacao B.V.

KYC Policy

Date: 23 April 2026

Version 1.0

1. Purpose

This KYC Policy (the “Policy”) sets out the framework by which Breckenridge Curacao B.V. (the “Company”) identifies, verifies, and monitors its customers and counterparties. The primary objective is to ensure that the Company maintains a robust understanding of the individuals and entities with whom it engages, thereby preventing the misuse of its services for money laundering, terrorist financing, or other illicit purposes. The Policy also ensures that the Company meets its regulatory obligations and safeguards its operational and reputational integrity.

2. Scope of Application

The Policy applies across three distinct but interrelated areas of the Company’s operations:

- a) all customers (players) who register accounts and transact on the Company’s platform.
- b) third parties with whom the Company establishes business relationships, including payment service providers, game providers, and other suppliers.
- c) internal and corporate structures, including directors and ultimate beneficial owners, particularly in the context of group oversight and incoming due diligence requests.

This unified approach ensures that the Company maintains a consistent standard of identification and verification across all relationships, rather than limiting KYC obligations to customers alone.

3. KYC Framework and Lifecycle

The Company adopts a lifecycle approach to KYC. Identification begins at the point of registration, where core personal data is collected. Verification is subsequently triggered either upon the customer reaching defined transactional thresholds or earlier where risk indicators arise. Once verified, customers remain subject to ongoing monitoring, with periodic reassessments conducted where necessary. Where higher risks are identified, enhanced due diligence measures are applied. This process continues throughout the duration of the



relationship and concludes only upon account closure, at which point records are retained in accordance with applicable requirements.

This lifecycle approach is mirrored, in a proportionate manner, in the Company's treatment of third-party relationships.

4. Customer Identification and Verification

At the point of registration, the Company collects key identifying information from customers, including their full name, date and place of birth, nationality, and residential address. This information forms the basis of the customer profile and is used both for verification and for subsequent monitoring.

Verification of identity is conducted through the collection of reliable and independent documentation. Acceptable forms of identification include government-issued documents such as passports, national identity cards, or driving licences. Verification of residential address is carried out through supporting documentation that demonstrates a clear link between the individual and their declared address. Such documentation typically includes utility bills, bank statements, or official correspondence issued by governmental authorities. Documents that do not reliably evidence residency, such as mobile phone bills or documents linked to non-residential addresses, are not accepted. These standards are consistent with those applied in the Company's third-party due diligence processes .

Verification is not always immediate upon registration. Instead, it is performed in line with a risk-based approach, most notably when a customer reaches a cumulative deposit threshold of €2,000 or where other risk indicators are present. Upon reaching this threshold, customers are required to submit the necessary documentation. Where documentation is not provided within the defined timeframe, the Company may restrict account functionality, including the ability to withdraw funds, and may ultimately suspend or terminate the account.

5. Ongoing Monitoring and Risk Assessment

KYC does not end at verification. The Company conducts continuous monitoring of customer activity to ensure that behaviour remains consistent with the information held on file. This includes analysing transaction patterns, gameplay behaviour, and payment methods used. Monitoring is both automated and manual, and is supplemented by external intelligence checks where appropriate.

Customers are assessed on a risk basis, considering factors such as geographical exposure, transactional behaviour, and product usage. Where a customer's risk profile changes,



additional verification or enhanced due diligence may be required. This ensures that the Company's understanding of its customers remains accurate over time.

6. Politically Exposed Persons and Sanctions

The Company maintains specific procedures for identifying and managing politically exposed persons ("PEP"). Where a customer is identified as a PEP, the relationship is subject to enhanced scrutiny. Additional information is obtained, particularly in relation to the source of funds and source of wealth, and any decision to continue the relationship is subject to approval at senior compliance level.

Similarly, all customers are screened against relevant sanctions lists at onboarding and on an ongoing basis. These include international and regional sanctions frameworks such as those issued by the United Nations and the European Union. Where a potential match is identified, the account is immediately restricted and escalated internally for review. Confirmed matches result in appropriate action, including reporting to the relevant authorities where required.

7. Third-Party Due Diligence

The Company applies comparable KYC standards to its third-party relationships. This includes payment service providers, game suppliers, and other operational partners. Before entering into a relationship, the Company conducts due diligence to understand the legal status, ownership structure, and regulatory standing of the counterparty.

For corporate entities, this involves obtaining incorporation documents, constitutional documents, and evidence of good standing. The Company also identifies and verifies ultimate beneficial owners holding a significant ownership interest, typically defined as 25% or more. Directors are also subject to verification, with the number of individuals reviewed determined on a risk-sensitive basis. These requirements align with the Company's established due diligence procedures.

In addition to documentary verification, the Company conducts independent checks, including open-source intelligence searches and database screenings, to identify any adverse information. Where a third party is regulated, the validity of its licence is independently confirmed through official sources.

Once onboarded, third parties are not treated as static relationships. They are subject to periodic review, typically on a biennial basis, and are reassessed where new risks emerge. This ensures that the Company maintains an up-to-date understanding of its business partners.



8. Incoming Due Diligence

The Company is frequently subject to due diligence requests from third parties, particularly in the context of payment processing and supplier onboarding. In such cases, the provision of corporate and ownership information is coordinated centrally by the Compliance Team. Documentation is shared through controlled channels, and records of all disclosures are retained. This ensures consistency in the information provided and maintains an audit trail of all external requests.

9. Escalation and Suspicious Activity

Where concerns arise during KYC or ongoing monitoring, these are escalated internally without delay. The Company's Money Laundering Reporting Officer (MLRO) is responsible for assessing such cases and determining whether further action is required. Where there are reasonable grounds for suspicion, a report is submitted to the relevant financial intelligence unit.

All employees are required to maintain strict confidentiality in such cases. Under no circumstances may the existence of a suspicion be disclosed to the customer or third party concerned.

10. Record Keeping

The Company maintains comprehensive records of all KYC activities. This includes identification documents, verification evidence, screening results, risk assessments, and any decisions taken in relation to customer or third-party relationships. Records are stored securely within the Company's systems, including dedicated due diligence repositories, and are retained for the period required under applicable laws and internal policies.

11. Governance and Review

This Policy is owned by the Compliance function and is subject to periodic review to ensure that it remains aligned with regulatory expectations and operational practices. Reviews are conducted at least annually, and more frequently where material changes occur in the regulatory landscape or in the Company's business model. Any updates are subject to appropriate internal approval