
Re: EveryMatrix KYC Policy

To whom it concerns,

As a B2B critical gaming supplier, EveryMatrix is not a relevant person in terms of applicable Anti-Money Laundering and Financing of Terrorism legislation.

Notwithstanding the preceding statement, EveryMatrix still employs a comprehensive AML/KYC as best practice at its discretion rather than by means of legal requirements.

With respect to your request concerning EveryMatrix's AML/KYC policy, specifically in relation to:

- Customer identification (KYC)
- Verification (CDD)
- Ongoing Monitoring
- Record Keeping

The undersigned, on behalf of EveryMatrix, as the designated *Money Laundering Reporting Officer* ("MLRO") provides as follows:

1. Customer identification and verification

The Customer Onboarding Process is initiated when a potential business relationship with a customer reaches the *Contract Stage*. During the *Contract Stage*, Due Diligence is performed with the purpose of:

1. Identifying and verifying the applicable Beneficial Owners (BOs)¹ in line with jurisdictional requirements and best practice.
2. Clarifying the intended nature of the business relationship in order to establish the Risk Profile of the entity and determine the appropriate risk mitigating measures.
3. Assessing the appropriate ongoing monitoring measures used to identify unusual transactions which may involve ML/TF.

¹ For the avoidance of doubt, for the purpose of this policy, a Beneficial Owner is defined as an individual which, whether directly or indirectly, owns 25% or more of the contracting entity. This % falls to 10% when onboarding clients subjected to enhanced due diligence procedures.

The following procedure is performed by the Compliance department on customers onboarded:

STEP	PROCEDURE
1	The Compliance department are introduced by the Sales Manager to the new Customer and its representatives.
2	The Compliance department forwards to the new Customer the CDD questionnaire.
3	The representatives of the Customer submit the questionnaire to the Compliance department. The Compliance department reviews the questionnaire and assign a risk scoring in accordance with the Customer Risk Assessment as approved by the Board.
4	Simultaneous to the preceding step, the natural and legal persons identified in the questionnaire are subjected to a PEP/Sanction/Adverse Media screening on the group's monitoring software. The natural and legal persons identified are also entered into the monitoring software's <i>Ongoing Monitoring Population</i>, whereby a passive PEP/Sanction/Adverse Media screening is carried out monthly and any hits reviewed. Any hits are documented in the Customer File accordingly. False positive hits are noted and an explanation for the <i>false positive</i> tag is noted. True positive hits are escalated to the MLRO. The MLRO reviews the situation, and after consulting official guidance notes and best practice measures, determines the way forward. This could be a request for additional documentation, escalation to C-level Management for approval to proceed with the business relationship, simple clarifications, or ceasing the relationship with the customer.
5	If the Compliance department, after the information gathered in steps 3 and 4, do not deem the risk scoring as representative of the information submitted, the MLRO is notified accordingly. The MLRO, will then, determine if the risk score is adequate or otherwise, and shall document the reasoning for retaining or amending the score accordingly in the Customer File accordingly.
7	Based on the final scoring, the Compliance department shall request the appropriate documents required in accordance with the score. If the final score shows a medium risk, normal CDD is carried out on the customer. If the score is categorised as high risk, then the customer is subjected to EDD. Should any of the variables be scored as ' <i>Extreme Risk</i> ', then the overall customer risk score is assumed to be beyond EveryMatrix's risk appetite, automatically leading to the Compliance department recommending that the potential business relationship is not pursued.
8	The documents are received and verified by the Compliance department. Any clarifications are handled. The Compliance department either recommends the customer for approval or refusal. Before recommending for approval, the Compliance department performs additional checks on the signed contract to exclude any unauthorised signature. If the latter is found, additional requests will follow to ensure a POA or any other document is provided.

Additionally, for customers that operate exclusively in one or more regulated markets in which both EveryMatrix and said customer both have a license for each applicable market; if such license allows, by virtue of best practices or regulation, and after obtaining the necessary legal advice for that specific market the procedure shall be deemed complete at step 5².

² In closed loop licencing systems, the Regulator accepts that both the supplier and client went through significant scrutiny to be onboarded and are monitored adequately by the Regulator. In this regard, the need for a supplier to carry out full KYC on a client is not required. EveryMatrix employs such practice only in top tier jurisdictions in Europe and North America, in jurisdictions where the veracity of a licence can be independently verified by the Regulator.

2. Ongoing Monitoring

The onboarding customer process provides EveryMatrix with a snapshot of the customer's risk profile. Risk, is however, dynamic, and over time due to certain events materialising, the customer risk assessment becomes invalid and will need to be updated.

The below is a non-exhaustive list of events which may alter the customer risk profile:

- Adverse media on any natural or legal person connected with the customer
- A natural person connected with the customer becomes a PEP
- A natural or legal person connected with the customer becomes subject to sanctions
- Material changes to the shareholding of the customer, specifically a change in the beneficial ownership^[5]
- Material changes to the corporate structure of the customer
- Changes to the Directors and other key personnel of the customer
- Listing or delisting on a stock exchange.
- A natural or legal person connected with the customer resides/is incorporated in a high-risk jurisdiction.
- The customer starts targeting players residing in a high-risk jurisdiction.

It is imperative to note that in the event of suspicions that any natural or legal person connected with the customer is carrying out ML/FT, such suspicions does not warrant a simple change in the risk profile but must be immediately reported to the applicable FIU(s), as required by money laundering legislation, regardless of EveryMatrix not being considered as a relevant person in terms of such laws.

The Group carries out two separate Ongoing Monitoring procedures as follows:

- Passive Monthly PEP/Sanction/Adverse media screening
- Notifications by customers on material changes

Passive Monthly PEP/Sanction/Adverse media screening:

Upon the Compliance department being made aware of a potential customer onboarding, the Compliance department immediately runs the:

- Contracting Party
- Related Companies (if applicable)
- Parent Company
- Beneficial Owners
- Directors
- Authorised Signatories

Through a PEP/Sanction/Adverse media screening. Such screening is then marked to automatically be carried out on a monthly basis. The Compliance department routinely reviews such screening, following the below procedure:

STEP	PROCEDURE
1	On a monthly basis, automatic PEP/Sanction/Adverse media screening on the customer population of the group.
2	Hits are reviewed accordingly and marked as either <i>False Positives</i> or <i>True Positives</i> .
3	False positive hits are marked so accordingly, specifying the rationale why (e.g. different person, adverse media not being particularly adverse, person holding office but not identified as a PEP in their country of origin and/or residence). True positive hits are raised to the MLRO for obtaining senior management approval in case of PEP.
4	The MLRO reviews the hit and determines the appropriate way forward. If the risk is acceptable, the MLRO will advise the continuation of the business relationship; if the risk is not currently acceptable, but can be mitigated to an acceptable level, then the MLRO will provide recommendations to ensure that business relationship can continue; if the risk is not currently acceptable, and can in no way, shape or form be mitigated to an acceptable level, the MLRO will advise the termination of the business relationship.

Notifications by customers on material changes procedure:

As per standard contract, customers are required to provide prior written notification on material changes. In practice this is highly difficult to enforce.

To this end, on an annual basis, the Compliance department sends an automatic link to all customers to confirm or otherwise, that no changes in line with events which may alter the customer risk profile as delineated earlier in this letter took place.

Should a customer inform EveryMatrix of material changes, the Compliance department shall conduct, partially or in full, the Customer onboarding process, as the case may be.

If a customer fails to reply to EveryMatrix's requests within 90 days of first notification, the Compliance department shall conduct an OSINT review according to the exigencies of the customer, escalating to Senior Management as necessary.

3. Record keeping

All information, documentation and KYC-related communication submitted by clients is kept by EveryMatrix in electronic fashion within its dedicated repositories as per company's policies and procedures.

Content and information access and sharing are restricted on a need-to-know basis in compliance with company's ISO 27001 certification requirements. Additionally, user rights (editing and/or viewing) vis-a-vis relevant content and information are set based on information and content classification as per company's policies.

In compliance with applicable legal requirements (as highlighted within company's applicable data retention policies) and the fair retention of personal data principle as encapsulated by art.5 GDPR, documentation is kept for a minimum of 5 years after termination of the supplier-client relationship.

At the five-year mark, the Compliance team reviews the documentation for validity and identify potential actions to be undertaken with respect to the relevant content and information at stake, including, without limitation, further retention, deletion, correction.

Yours Sincerely,

Jake Cachia Manicolo
Compliance & AML Manager, MLRO
EveryMatrix