ANTI MONEY LAUNDERING AND COUNTER TERRORISM FINANCING POLICIES AND PROCEDURES

Introduction

The company Meridian Gaming Ltd establishes and maintains the policies and procedures in relation to prevention of money laundering and funding of terrorism. The company is committed to conducting its business operations in line with the laws and regulations applicable in Malta in regards to the Anti Money Laundering and Terrorist Financing, such as the Prevention of Money Laundering Act (Cap. 373 of the Laws of Malta), Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR S.L. 373.01), Implementing Procedures Part I on the Prevention of Money Laundering and Funding of Terrorism published by the Financial Intelligence Analysis Unit, last amended on 18th October 2021 and Implementing Procedures Part II published by the Financial Intelligence Analysis Unit and the Malta Gaming Authority revised on 2nd July 2020.

The company Meridian Gaming Ltd establishes and maintains the policies and procedures in relation to prevention of money laundering and funding of terrorism. These policies and procedures are implementing the risk based approach in operating as a B2C licensee, in relation to establishing and handling the business relationship with customers.

Money Laundering Reporting Officer

Meridian Gaming has appointed a Money Laundering Reporting Officer (MLRO) with sufficient seniority and command to perform his duty.

The details of the MLRO are as follows:

Name: Natalija Dutina Vranka
Contact email: natalija.dutina@meridianbet.com
Phone number: +381668010132

MLRO has the responsibility to review internal reports, suspicious transactions, players' risk scoring and to file Suspicious Transaction Reports.

The MLRO is the main contact in communication between the Company and the FIAU.

All employees of the Company are aware of the identity of their MLRO and the deputy MLRO and how they can be contacted as well as the procedure for reporting.

The MLRO can be contacted directly, and the Company has also arranged an anonymous channel so all employees can contact the MLRO and inform him about activities they found suspicious.

MLRO is responsible for:

- Receiving and reviewing internal reports relating to the prevention of money laundering and countering terrorist financing
- Responding to the requests made by FIAU in relation to the prevention of money laundering and countering terrorist financing
- Reviewing suspicious transactions and the player risk scoring and managing internal AML software
- Making decisions about filing and afterwards filing the STRS to the Financial Intelligence Analysis Unit
- Implementing, managing and controlling the AML policies, procedures and controls within the Company
- Making reports to senior management on anti-money laundering (AML) and countering terrorist financing
- Providing, organizing and monitoring of AML related trainings to the relevant staff

The MLRO has the authority and seniority to act independently in carrying out his responsibilities, and access to sufficient resources to carry out the duties. The MLRO has sufficient time to dedicate himself and perform his duties.

The training of the relevant staff is further explained in the document AML/CFT Training Policy.

Business Risk Assessment (BRA)

The Company has hired the company ARQ Group Malta to perform the Business Risk Assessment.

The carried out Business Risk Assessment provides a detailed analysis of the ML/FT risks associated with the Company's products, payment methods accepted, transactions processed and the customer base of the Company.

The qualitative and quantitative factors such as the conclusions of the EU Supranational Risk Assessment (SNRA), the National Risk Assessment (NRA), and reports and guidance documents published by the Financial Action Task Force have also been considered in conducting the BRA: The controls put in place by the Company to mitigate the possibility that such risks to materialize have also been assessed for their effectiveness and to determine the residual risk of the Company.

The aspects in completion of the BRA inter alia were:

- The exposure to the inherent risk in regards to the customers, games offered, jurisdiction analysis, delivery channels and payment methods

- Identification and analysis of AML/CFT controls deployed by the company

- Determination and quantification of the residual risk

The methodology applied is further described in the Business Risk Assessment document V1, completed in March 2021, and approved by Shareholder's resolution on 10th April 2021.

The Business Risk Assessment is revised at least once a year and is approved by the shareholders' resolution.

In case there are significant changes in the scope of the company's business activities and environment such as expanding the customer base, new addition to the games offered or new payment method added, changing the structure or organizational scheme in the company, the Business Risk Assessment should be updated accordingly.

Customer Risk Assessment

The Company has developed an in-house Customer Risk Assessment software, that automatically checks each player upon registration on the meridianbet.com website and sets the initial risk scoring which is later modified in accordance to the player's level of play, activity and personal information available. The CRA takes into consideration Customer Risk, Country Risk, Payment Method Risk, Product/Service Risk, Transaction Risk and Interface Risk, and each player gets an initial score once they register to the website. The software automatically collects data from the registration form, and automatically gives out a score based on the information available at that stage, and places the customer in the relevant risk category. Besides that, the software takes into consideration other information on the player collected during the business relationship, such as data collected in the Customer Declaration form, data from the EDD procedures and other data received from searches from the reliable sources done by the AML team.

The risk categories the Company recognizes are:

1. Low risk
2. Medium low risk
3. Medium risk
4. Medium high risk
5. High risk

The scoring of the risk factors, CRA ranges for each risk category and the specifications of the AML/CFT software is further explained in the Customer Acceptance Policy and Customer Risk Assessment Methodology Document.

Customer risk

Customer risk is the risk of ML/FT that arises from entertaining relations with a given customer. Determining the potential money laundering and terrorist financing risks posed by a customer, or category of customers, is critical to the development and implementation of an overall risk-based framework. The Company seeks to determine whether a particular customer poses a higher risk and the potential impact of any mitigating factors on that assessment. Application of risk variables may mitigate or exacerbate the risk assessment:

Categories of customers whose activities may indicate a higher risk include:

- customers who are PEPs, family members of PEPs or known close associates of PEPs
- high spenders or disproportionate spenders
- regular customers with changing or unusual spending patterns
- occupation – The customer work in a cash-based environment
- employment status – The customers that are not employed or work part time pose a higher risk
- reluctance to provide CDD documents
- connections to sanction lists
- criminal and Non-Criminal Adverse media connected to the customer
    - Adverse media represents any kind of unfavorable information found across various of news sources. It is important to note that adverse information does not have to be proven facts to be considered relevant. Suspicions and allegations of crimes are worth taking into account to avoid association
    - Examples of adverse media sources that can be used for checking are:
    - Traditional news sources and media;
    - Databases of international organizations;
    - Blogs and web articles, including websites that publish issues involving corruption, rackets, and financial fraud;
    - Social media and internet.
    - Checking for adverse media is the process of screening a client against news articles, legal prosecution or similar content that may affect the customer's final risk by revealing their involvement in money laundering, terrorism, fraud, tax evasion, or other types of crimes. This is a part of our regular ongoing customer risk assessment procedure. We also apply the searches when increasing the quantity of information obtained for CDD purposes

Country and geographical risk

Some countries pose an inherently higher money laundering and terrorist financing risk than others. In addition to considering their own experiences, the Company takes into account a variety of other credible sources of information identifying countries with risk factors in order to determine that a country and customers from that country pose a higher risk. The company takes into consideration the following lists: FATF black list, FATF grey list, EU list of high-risk jurisdictions, OFAC sanction list, MONEYVAL and all other relevant lists that can provide a better insight into the country of the customer.

When determining the risk, the company takes into consideration the following:

- Nationality/Citizenship
- Country of Permanent Residence
- Country of source of income
- Country of source of Funds
- Link to non-reputable jurisdictions

The list of jurisdictions, and the score that each country holds can be seen in the "CRA Risk Matrix" document.

Payment/transaction risk

The Company has in its general offer on the website a variety of payment methods that a customer can use at all time. The methods vary from credit/debit cards to e-wallets and vouchers. The multiple use of all payment methods can point to a higher risk behavior given that the customer is trying to hide the trace of these transactions. The opening of such online payment accounts is usually much easier than opening a standard bank account, with fewer KYC checks and AML procedures.

The Company always uses payment methods and payment providers that are regulated within the EU, and licensed within the EU, and does not use third party payment processors.

When determining the payment risk of the customer, the company looks at the following instances:

- Payment method used:

1. Credit/debit card
2. Bank transfer
3. E-wallet (Skrill or Neteller)
4. Voucher (Neosurf)
5. Cash payments

- Multiple payments used, three or more payment methods used pose a higher risk

The Company imposed certain payment limitations on all customers, limits by payment method and a maximum daily limit. The limits can be waived if the customer is assessed with a low to medium risk rating, and if the full CDD measures were honored.

The Company as a both retail and remote gambling operator, acknowledges the risks deriving from cash transactions in its retail outlets. Such transactions are automatically considered as higher risk than transactions that are done through other payment methods.

To mitigate the cash-based risk in betting shops, the Company introduced POS terminals, and encourages the customers to deposit and play with the use of credit/debit cards, in order to maintain a lower cash inflow.

Product/Interface Risk

The Company acknowledges that certain games offered may pose a higher/lower threat of ML/TF. Meridian Gaming ltd offers a variety of online casino and online sports betting games to players, and categorizes the risk by the game itself.

The games offered are grouped by their category type as follows:

- Table games
- Live casino games
- Slots
- Sports betting

The risk rating of the mentioned games is as follows:

Games	**Risk**
Slots	Low
Table games	Low
Live Casino	Medium
Sports Betting	Medium

Besides the risk rating of the game aka the product, the company recognizes the risk of non-face-to-face business relationship with its customers. Since the company offers remote gambling services, so the customers are met in person, and they are not physically present for the verification process, the inherent risk posed by this kind of business relation is higher than the business that the company has in its retail outlets.

The retail business, through betting shops, offers games such as:

- Slots, via self-service betting terminals
- Sports betting, both over the counter and via self-service betting terminals

By the rating of the customer risk, the company takes into consideration the fact that some players are both customers in betting shops and on the website, therefore the presence of the customer is known to the company in the end.

Customer Due Diligence (CDD)

In applying the CDD measures, the company has a goal to build the customer profile and in accordance to that further establish the customer's risk rating as a part of the customer risk assessment.

The level of the CDD measures to be applied to the particular customer in the particular moment of customer's journey is established in accordance with the information available to the company about the customer, in regards to his/her activity and personal information.

Identification and Verification

The first contact with a customer begins at the registration stage, when a customer creates a player's profile on meridianbet.com website/application.
During the registration, a customer fills in certain personal information in order to be identified by the company. A customer can only have one account on meridianbet.com website.

Personal information collected at the stage of registration is:

- First and Last name
- Date of Birth
- Country of residence
- Permanent residential address
- Phone number and email
- Gender

After a player completes the registration form and is identified, the provided information must be confirmed in the verification stage.

After registration, a player receives an email in which he/she is invited to complete the verification process by providing the company with the documents sufficient to prove his/her identity and the permanent residential address.

As proof of identity the company accepts one of the following:

- Valid passport (full double-page)
- Valid identity card (both sides)
- Valid driving license (both sides)
- Valid official residence document

As proof of address the company accepts a full-page document of one of the following:

- Bank statement/confirmation
- Utility bill for services such as telephone, gas, water, electricity
- Residence certificate
- Any official document certified by local authorities

For the verification of the address, the company only accepts documents not older than 6 months from the day of their receipt.

Until the verification process is completed and the required documents provided by the players are checked by the Customer Support Department - manually and/or by using the GBG ID3global software to check the validity of a passport/ID card, players are not provided with the activation link. Without the activation link, the players cannot log into their accounts and therefore cannot deposit any funds nor place any bets.

Players also have the possibility to upload the necessary verification documents in the registration process, prior to receiving the verification email and in that case will receive the activation email after the Customer Support checks the validity and quality of the provided documents.

All the documents for verification purposes made available by the customer must be in good quality and all the information included in the documents must be clearly visible.

The first steps of establishing the player profile and appointing a risk rating are initiated in the registration stage, as the company's in-house AML/CFT Customer Risk Assessment Software takes into account the information provided by the player - such as country of residence.
After the verification stage is completed and more information on the players is known, this is used to further complete the player profile and assign the risk rating in accordance to the previously established risk factors and the scoring for each type of risk.

PEP and Sanction Screening

Meridian Gaming Limited uses the PEP and Sanction screening software, GBG ID3global.

The screening system allows the Company to keep track, monitor and spot politically exposed persons and individuals that are listed in sanction lists or have committed criminal offences.

The software takes into account the full name and date of birth and runs it through a vast database. The Company has integrated the screening tool, so that each and every player that registers on the website is screened automatically. The PEP and Sanction Screening is done in parallel with the player's registration process. Additionally, the PEP screening is repeated within the 30 days from the point at which a player reaches the threshold of 2.000 EUR in deposit, regardless of the fact that he/she was already screened for PEP status.

The results are sent via email immediately to the MLRO and the Customer Support department. If the player enters a wrong name, or misspells the name, the Customer Support department will (upon verification) change the name, and run it through the screening tool manually.

In case there is a match in the GBG ID3global software, the AML team, in accordance with the MLRO, performs a thorough research in online available databases to determine if the customer definitively is a match, or whether the customer has a similar name to the existing PEP.

Additionally, in the Customer Declaration Form, which is sent to customers when they are either risk rated as Medium Risk or have reached the 2.000 eur threshold in deposits, the players are additionally asked to make a declaration on whether they are Politically Exposed Persons or not.

In case the GBG ID3global software recognized a player as a PEP or found them on a Sanction list, this information is automatically shown in the company's in-house AML/CFT Customer Risk Assessment Software. The player instantly receives a high risk label, and if it is confirmed by the MRLO that the person recognized as a PEP in the GBG ID3global software is actually not the same player, the rating is manually changed by the MLRO.

In instances when a player declares himself as a PEP in the Customer Declaration Form or this information is acquired in another way, this information is manually added to the company's in-house AML/CFT Customer Risk Assessment Software and the player is rated as high risk.

In case the customer is a PEP, he/she is not allowed to place any deposits or bets until it is approved by the Board.
The Board approval is kept in writing. Additionally, the EDD is performed on the customer.

Purpose and Intended Nature of Business Relationship

When a customer reaches a threshold of 2.000 EUR (in a single, or multiple connected transactions) in deposit in the last six months of the player's activity, the company collects additional information from the player in order to establish his/her source of wealth and the expected level of play.

In cases when the player was risk rated as Medium in the company's in-house AML/CFT Customer Risk Assessment Software, this information is collected on the player prior to him/her reaching the 2.000 EUR threshold.

For the purpose of establishing customer business and risk profile, the player is asked to complete the Customer Declaration Form consisting of the following necessary fields, apart from personal details:

- Nationality and any former nationalities
- Identification number and date of expiry of the ID document

Information to establish customer's source of wealth:

- Employment status
- Occupation/former occupation
- Annual Income - gross income from their employment
- Other source of income

The information about the expected expenditure on the company's website/application:

- Expected amount to be spent for play in a month's period
- Whether the player's monthly income adequate to cover the expenditure
- Usual frequency when visiting gambling websites

They will also need to sign the form manually and agree to our Terms & Conditions and the Privacy Policy before submitting it.

The form is currently located on a link specifically created for it, and is sent to players via email.

After the customer is asked to complete the Customer Declaration form, he/she has 30 days to provide the company with the required data. During that period players will be able to use their accounts and the website as usual, however, they will not be allowed to make any withdrawals until we have received the completed form.

If a customer provides incomplete or incorrect data (compared to information saved in our database), the form will be resent to them with a request for resubmission, while details as to which information exactly is needed will be given in the email.

In the instances when the required documentation is not submitted in the provided deadline, the customer's account is suspended and the MLRO decides in every particular case on whether an STR should be submitted to the FIAU, based on the customer's risk rating.

In case the risk rating is Medium and the MLRO deems that there are no suspicious activities or transactions from the customer, and the customer has funds on account, the funds are returned to the customer in the same way they were deposited, or if that is not possible, the player is contacted to provide information on where the funds should be sent.

The MLRO and the AML team can use other available sources of information to complete the customer's profile, such as social media, newspaper information, available open databases etc.

Additionally, to complete the customer's profile, the statistical data from the website for the customers that are originating from the same jurisdictions and/or have similar activity on the website, can be taken into account.

The information acquired from the player is added to the company's in-house AML/CFT Customer Risk Assessment Software in order for the appropriate risk rating to be established for the player.

Authentication of the documents

In the GBG ID3global software, used by the company to check if a player is a PEP or on Sanction lists, there is a feature that allows the Company to check the validity of documents provided by the player - passport or ID.

The company only accepts the CDD documents in the non-modifiable format such as PDF, PNG, JPG etc. Word format and any other format that can be easily modified is not accepted.

All documents provided by the player are checked manually by the members of the Customer Support team.

In addition to GBG ID3global software, the members of Customer Support team and the AML team use other available sources to confirm the validity of provided identification documents:

- www.edisontd.net;
- https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/borders-and-visas/schengen/docs/handbook-annex_23_part_1_and_2.pdf;
- https://www.consilium.europa.eu/prado/EN/prado-start-page.html.

All additional searches performed on the player are kept alongside other personal information provided by the player.

Translation of the documents

The main language in which the company employees are communicating with the customers and all the documents and forms made available to the customer are in English language.

Besides English, the company employees, including the ones employed in the Customer Support department, are familiar with Serbian, Bosnian, Croatian, Montenegrin languages, as well.

All the documentation provided by the customer which is not in a language known to the employee of the Customer Support department shall be translated to the English language in writing and the copies of the translation shall be kept in the customer's file, alongside the original document.

Ongoing Monitoring

In carrying out on-going monitoring of a business relationship, the Company works closely with all relevant departments to:

1. Ensure that the documents, data or information held are kept up-to-date

The Customer Support department follows and writes in the customer card the expiry date of the document. The system sends out a notification to the Customer Support department warning them that the document is soon to expire. The player is requested to send the new document, and if they decline, the business relationship should be terminated

2. Follow the consistency of the transactions undertaken throughout the business relationship

The Company follows the players lifeline and makes sure that the player is playing within his/her already provided confirmations of the nature of the business relationship. If there are some changes in the behavior or expenditure, the player will have to provide additional documents to prove the new gaming pattern

3. Regularly revise the players PEP status

The fact that the player is not a PEP at the beginning of the business relationship can change in time. The monitoring must be done in order to always stay on top of certain changes in the status, either of the player or his close family and connections

The level of on-going monitoring will depend on the risk profile of the customer, however, the Company will still in some degree monitor the player that is deemed a low risk category, to ensure that the business relationship still warrants to be considered as a low risk one. A change in circumstances may lead to an eventual re-evaluation of the risk, noticed by the CRA software, or any other relevant department.

Account closure and players' funds

In case a customer's account is closed, for whichever reason, all the remaining funds on the account will be returned to the customer the same way they were deposited. Should this not be possible, the Company will ask the player to provide an alternative way and will do all necessary checks to verify that such

payment channel belongs to the same player, and there is no suspicion of fraud or money laundering activities.

It should be emphasized that all funds deposited by the player will be credited to the player's account only.

The customers' transaction data kept on file includes the following details: fist name, last name, player ID, date, time, amount, payment method, unique transaction ID.

Additionally, the Company's system is able to generate a dated and timed report and any point in time, containing the data listed below:

- The aggregate cashable balances in the players' accounts (by currency);
- Open bets/chips in play/participation fees forming part of an open prize pool (by currency); and
- Unprocessed withdrawals which have been deducted from the player's cashable balance but have not yet been returned by the Company to the respective player's wallet/bank/card

A customer's account will be deemed inactive (dormant) if none of the following actions takes place by the account holder in the consecutive period of 12 months: making deposits, using the bonus, placing a bet, playing casino games, requesting a withdrawal, in spite of the fact that a player had been notified on the forthcoming inactivity of their account 30 days before the account is due to become inactive. After the lapse of 30 days from the notification to the player that the account will be declared and treated as inactive with the consequences thereof, the Company starts charging the inactivity fee of €5 per month, of which the player is informed again.

Enhanced Due Diligence

In cases when the customer is deemed as high risk in the company's in-house AML/CFT Customer Risk Assessment Software, the customer is asked to complete the Enhanced Due Diligence form in order for the company to acquire more information about the player and mitigate the risk recognized by the software.

It is important for the Company to verify the source of funds or wealth involved in the business relationship, and to be fully aware that the funds do not come from the proceedings of crime. Within the EDD form, the player needs to confirm his intended nature of the business relationship, especially to confirm that the intended funds to be spent in the said business relationship is in the lines of his/her expenditure and pay grade.

The EDD form helps the Company to get unanimous confirmation about the employment status and the occupation of the player, by asking from the player to send one of the following documents:

- Employment income statement
- Past three months' wage slips
- Letter from employer confirming salary
- Bank account statements showing last three months' salary payments, or if self-employed: recent, complete audited accounts or a completed tax return

If the player uses multiple payment methods and constantly changes the payment method for depositing, followed by a chargeback request from the payment provider, Enhanced Due Diligence must be applied as an additional measure to counteract this transaction risk.

In the EDD procedure, to be certain that the ID document the player has sent is legitimate, the player is requested to send a picture of himself/herself holding the said document. This request may come earlier if the player sent over a document with a poor quality.

In the instances when the required documentation is not submitted in the provided deadline, the customer's account is suspended and the MLRO decides in every particular case on whether an STR should be submitted to the FIAU, based on the customer's risk rating.

Suspicious Transaction Report

The main responsibility of the MLRO is to consider any internal reports of unusual or suspicious transactions and, where necessary, follow up on the same by filing a Suspicious Transaction Report (''STR'') with the FIAU. FIAU considers the MLRO to be the main contact point within the subject person and he is to act as the main channel through which any communications with the FIAU are to be conducted.

Procedures for reporting suspicious transactions

Suspicious transactions identified by relevant departments will be reported to the MLRO, which will assess and further examine the case and keep the findings available in the Company Fraud Folder.

The employees are informed and trained that tipping off players about the following situations is strictly forbidden:

- a submission of an STR to the FIAU, regardless of the subject of the report
- information requested by or provided to the FIAU, related to the ML/FT matters
- a suspicious customer and/or situation that is being investigated due to ML/FT concerns.

The MLRO will review the transactions, the customer's account history, the player's risk rating, the reports made about the player from the Risk Department and any other relevant information, and where he considers that there are sufficient indicators that money laundering/terrorist financing may be taking place, he will pass the information directly to the FIAU in the procedure established by that institution.

The following is a list of possible red flags which will be to considered:

- Customer does not cooperate in carrying of CDD.
- Customer attempts to register more than one account on the operator's website
- Customer deposits funds well in excess of what is required to sustain his/her usual betting patterns.
- Customer makes small wagers even though he has significant amounts deposited, followed by a request to withdraw well in excess of any winnings.
- Customer makes frequent deposits and withdrawal requests without any reasonable explanation.

- Noticeable changes in the gaming patterns of a customer, such as when the customer carries out transactions that are significantly larger in volume when compared to the transactions he normally carries out.
- Customer enquiries about the possibility of moving funds between accounts belonging to the same gaming group.
- Customer carries out transactions which seem to be disproportionate to his wealth, known income or financial situation.
- Customer seeks to transfer funds to the account of another customer or to a bank account held in the name of a third party.

Meridian Gaming has a documented process in place for all its employees to report when they have suspicions that a customer may be engaged in money laundering or terrorist financing to the money laundering reporting officer (MLRO).

Where suspicious transactions are identified, the account will be suspended until further notice by the FIAU (i.e. the customer will be unable to log into the account and will be advised to contact the Customer Support Team).

A register will be maintained which includes the details of all enquiries made by the authorities or the reports made to the authorities.

Record Keeping

The company's record keeping policy and procedure covers records in the following areas:

- MLRO's reports to senior management;
- Customer identification and verification information;
- Supporting records in respect of business relationships and monitoring of the customer's transactions;
- Employee screening records: all employees are required to obtain and provide to the Company a recent police conduct (not older than 6 months)
- Employee training records, specifically:
- AML yearly training
- Training of employees within departments
- External educations for employees
- Internal trainings for new products and/or programs
- Internal and external suspicious activity reports;

The data concerning training records which is being kept is: first name, last name, date and type of training conducted, as well as a short overview of the topics covered.

All documentation is kept for at least 5 years from the date on which the business relationship is terminated. When the exact date of a business relationship termination could not be determined, the 5-year period commences on the date on which the last transaction in the course of that business relationship was carried out. More recent paper documentation is stored at highly monitored premises of the office, and older records are stored in a secure location and kept in a register so that it is retrievable

on authorized request. The electronic data is kept in accordance with Information Security Policy and Data Security Policy, which are in line with the requirements of the General Data Protection Regulation.

Policy Review

The Company shall, at least once a year, re-inspect whether there is any material change in applicable regulatory framework implicating the revision of this Policy.

Signed on 23.11.2023.by

Natalija Dutina Vranka, MLRO

Stefan Pavlovic, CEO of Meridian Gaming Ltd