HELLENIC LOTTERIES S.A.

Policy on Anti-money Laundering and Countering Terrorist Financing (AML/CTF)

CONTENTS

1. Introduction

1.1 Definitions - Glossary

Some of the main terms and abbreviations used in the present Policy are interpreted as follows *(to facilitate immediate access).* The Regulation *(HGC Decision no. 554/5/15.4.2021)* and L. 4557/2018, as in force, include a detailed explanation of additional terms and concepts used in the Policy.

Authorities: Any state Authority related in any way to Hellenic Lotteries S.A.'s object of activity and the financial crime, such as indicatively the Ministry of Finance, the Independent Authority for Public Revenue *(AADE)*, the Financial Police, the Hellenic Police Headquarters and/or the regional police directorates.

The Hellenic Financial Intelligence Unit: The Hellenic Financial Intelligence Unit of article 47 of L. 4557/2018.

HGC: The Hellenic Gaming Commission.

Stakeholders: Stakeholders include the members of the Board of Directors, Unit Heads, Directors, Company Employees, physical network Agents *(e.g. OPAP Agencies)*, and other important internal/ external partners thereof *(e.g. leased Employees, important suppliers)*.

Business Relationship: The business, professional or commercial relationship, which is linked to the professional activities of Hellenic Lotteries S.A. and which is expected, at the time when the contact is established, to have an element of duration. Indicatively, a Business Relationship would be considered the conclusion of a contract with entities that constitute the Company's Physical Network.

Regulation: The *HGC* Decision under no. 554/5/15.4.2021, titled "Issuance of Regulation on the application of AML/CTF measures by Obliged Persons in the gaming market, pursuant to case f, par. 3, article 28 of L. 4002/2011 (A 180)".

Law against ML/TF: Law 4557/2018, "Prevention and suppression of money laundering and terrorist financing *(transposition of Directive (EU) 2015/849)* and other provisions".

ML/TF: Abbreviation of the term "Money laundering/ Terrorist Financing". The terms Money laundering and Legalization of Proceeds Generated from Illegal Activities have the same meaning.

Policy: The present Company policy on facing ML/TF risk.

Group AML Compliance Coordinator: In the case of OPAP Group, the AML Compliance Coordinator is the person appointed at a Group level *(in execution of the provisions of articles 36 and 38 of law 4557/2018)* to coordinate the activities of all Group Obliged Persons' AML Compliance Officers and to share relevant information therewith, as required.

AML Compliance Officer: The person appointed by each of OPAP Group's Obliged Persons to be responsible for AML/CTF. The specific person is appointed in said capacity by the Obliged Person, pursuant to article 4, and performs the duties of article 5 of HGC Decision 554/5/15.4.2021.

Obliged Person: The person Organizing or Conducting Games of Chance in the Greek Territory, including the Physical Network, as well as Casino Enterprises. In the case of OPAP Group, the Obliged Persons operating in the field of Games of Chance are OPAP S.A., Hellenic Lotteries S.A., and Horse Races S.A. Respectively, each member of the Physical Network of the aforementioned constitutes an Obliged Person.

Physical Network: OPAP S.A. Agencies, the land-based points of conduct of mutual horsebetting (*by draws or not)*, the land-based points of conduct of State Lotteries Games, wholesalers and retail sellers of State Lotteries and the Ultimate Beneficial Owners of all the aforementioned.

1.2 Objective

Hellenic Lotteries S.A. (*hereinafter the "Company"*) operates as a Gaming Provider *(organization and conduct)*, pursuant to the provisions of the relevant legal and regulatory framework. Acknowledging that its said operation makes it a potential gateway for funds of illicit origin channeled towards the legal economy, and given that it constitutes an Obliged Person pursuant to the Law, the Company has to apply and use appropriate structures and mechanisms to mitigate relevant risks.

In this context, the Company adopts the present Policy, which sets forth the required fundamental principles and rules to protect the Company itself, the Group to which it belongs, and in general, the financial/ transactional system from risks, which are related to ML/TF.

More specifically, under the present Policy, the business owner of which is the AML Compliance Officer of article 4 of HGC Decision 554/5/15.4.2021, the Company aims at:

- Establishing a single framework, which will be notified to Stakeholders via the appropriate means so that they all operate and respond in full alignment therewith,
- Ensuring its compliance with the from time to time requirements of the competent Supervisory Authorities,
- Supporting its strategic goal for sustainable and long-term development, through the protection of its integrity, credibility, and reputation against its eventual involvement in ML/TF incidents.

1.3 Legislative and Regulatory Framework

Achieving the Policy objective as such is described in the aforesaid chapter requires the integration and specialization via the Policy of the requirements of the from time to time applicable legislative and regulatory AML/CTF framework (*both internal and external*). The specific framework is currently consisted of the following main components:

- Law 4557/2018, "Prevention and suppression of money laundering and terrorist financing and other provisions", as recently amended (*under L. 4734/2020*) and in force from time to time.
- The Hellenic Gaming Commission (*HGC*) decision under no. 554/5/15.4.2021, "Issuance of Regulation on the application of AML/CTF measures by Obliged Persons in the gaming market, pursuant to case f, par. 3, article 28 of L. 4002/2022 (A 180)",

as in force from time to time, specifying and interpreting the foregoing law as in force in connection with its application by Obliged Persons in the Gaming sector,

- Ministerial Decision under no. 56591 ΕΞ 2021, having as its subject "Determination of duties and responsibilities of persons holding or having held a significant public office and arrangement of specific issues",
- The Company Board of Directors resolution on the appointment of an AML Compliance Officer, pursuant to article 38 of L.4557/2018 and article 4 of the aforesaid HGC 554/5/15.4.2021 decision.

1.4 Compliance with the Policy

Any failure/inability to comply with the provisions of the Policy could potentially lead to the Company's involvement in serious ML/TF incidents/events, subsequently resulting in (inter alia):

- Defamation of the Company and OPAP Group, with possibly negative consequences for its business continuity,
- Imposition of high pecuniary fines, penalties, and administrative sanctions to the Company,
- Impediment of Company strategic plans and objectives,
- Imposition of individual administrative and/or penalties and/or financial sanctions to Stakeholders.

In view of the above as well as the provisions of the legal framework, which categorizes/ recognizes the Company as an Obliged Person, **Compliance with the Policy is mandatory to all Stakeholders**, who commit to remain aligned therewith (*including any future versions thereof*) and do what is feasible for the prevention and suppression of ML/TF.

It is noted that the Stakeholders' undertaking to comply with the Policy is formally pursued by various means, which inter alia include a signed declaration of acceptance of the Group's Code of Conduct *(e.g. in the case of Personnel)* or the integration and signing of specific terms in the Company's contractual documents *(e.g. the Company's contracts with the Physical Network partners)*, whereas it is also achieved in practice thanks to the provided training on AML/CTF matters and the consistent application of the required controls and procedures, as the case may be.

1.5 Approval and Revision of Policy

Following a recommendation made by the AML Compliance Officer, the Company Board of Directors is the competent body to approve the present Policy and any required future amendments thereof that arise as a result of its ordinary or extraordinary review. Non-material amendments may take place upon the AML Compliance Officer's sole recommendation followed by the consent of the Chief Financial Officer under whom he/she falls *(or any other competent person/body that he'll be organizationally falling under in any future case)*.

The need to revise the Policy is subject to an annual assessment undertaken by the AML Compliance Officer to ensure its appropriateness and adequacy in relation to the nature, size and complexity of the activities, and the Company's risk profile in place from time to time. In order to implement the said assessment, the AML Compliance Officer indicatively takes into account the findings that may have derived from both internal and external (*e.g.*

the HGC) auditors' controls, the respective findings and events that derived during the year because of the activities of the Company's Special AML/CTF Service, as well as respective findings and information that derived from the AML Compliance Officers of the rest Group companies that hold the capacity of the Obliged Person.

Additionally, the need to have the Policy revised will be ad hoc reconsidered in the following cases:

- When significant changes take place to the organizational structure of the Company,
- When new products/ services are launched or when a material modification is made to existing products/ services,
- When amendments are ascertained to the relevant legislative/ regulatory framework,
- In any other case where the Company Management deems that such review and revision are necessary.

1.6 Notification of the Policy

The Policy, as a whole, is notified to all involved Company personnel, by being posted on the intranet portal or via e-mail or the use of any other suitable means, whereas, at the same time, the AML Compliance Officer sees to ensuring that a response is provided to any query relevant to the Policy and that training thereon is provided to the personnel involved.

Respectively, the Policy is notified to the land-based partners' Physical Network via the relevant OPAPNET portal *(in case of OPAP network Agents)* or via any other suitable means *(e.g. through email in the case of all non-opap Agents)*. Moreover, the Policy is posted on the Company corporate website to be accessed by all other stakeholders *(e.g. investors, consumers, creditors, suppliers, Agents that have not access to it / have not been notified through other means)*.

2. Governance, Description of Roles and Competences

2.1. Board of Directors

In pursuance of the provisions of the institutional framework in force, and further aiming both at its substantiated active participation in the management of the ML/TF risk and at conveying the appropriate message (*"The tone from the Top"*) and at instilling a relevant culture across the personnel and the Company's Physical Network partners in connection with the significance attributed to the effective management of the said risk, the Company's Board of Directors:

- Appoints, as per the provisions of sub-chapter 2.2, the AML Compliance Officer for the prevention and suppression of ML/TF, specifying his/her relevant duties.
- Ensures the independence of the aforesaid person, as well as his/her ability to access any information required for the performance of his/her duties.
- Provides the required protection (*physical, legal etc.*), pursuant to article 26 of the AML/CTF Law to the AML Compliance Officer, the Personnel falling under him/her, as well as to all the Stakeholders who report information on incidents and transactions eventually related to ML/TF.

- Sees to the provision of sufficient resources and assets (human resources, training budget, information and technology infrastructure), considering any relevant recommendations made by the AML Compliance Officer to ensure the effective performance of their duties.
- Based on the recommendations made by the AML Compliance Officer, approves the Policy and all the provisions thereof, as well as the relevant allocation of responsibilities regarding the prevention and suppression of ML/TF.
- Assesses and makes decisions, when so required, on relevant matters and risks (e.g. may resolve on or delegate the passing of the said resolutions relating to the termination of the relationships with customers or Physical Network agents deemed as unacceptable or of high-risk to other bodies) that derive and/or arise from the regular/ ad hoc reports, informational presentations and recommendations submitted by the AML Compliance Officer or other competent internal or external auditing bodies.

2.2. AML Compliance Officer and Group AML Compliance Coordinator

As per the aforementioned in sub-chapter 2.1, the Company Board of Directors is responsible for appointing the AML Compliance Officer, having as their main mission to pursue the adherence of the Company to all types of legislative/regulatory obligations on AML/CTF. By approving the present Policy, the Board of Directors authorizes the AML Compliance Officer to have full and seamless access to any information required for the performance of their duties. It also sets forth that the recipients of requests submitted by the AML Compliance Officer are obliged to forthwith respond thereto.

The AML Compliance Officer of the Company *(but also the staff of the Team that supports him/her)* may be a person who does not have a direct contractual relationship *(eg a salaried employment agreement)* with it. In particular, the Company can appoint as its AML Compliance Officer an Executive of the Group's parent company, with which a corresponding umbrella service contract has been drawn up, in the scope of which the relevant compliance services with the provisions of the relevant legal and regulatory framework of the HGC are included. In such cases, the appointed Executive may perform parallel, yet relevant tasks for the Company he/she is related with under a salaried employment agreement and the Group, inasmuch as those do not affect the efficiency of the performance of his/her duties being an AML Compliance Officer of Hellenic Lotteries S.A.

Furthermore, the appointment of the said Executive is finalized upon the granting of the relevant Suitability Authorization by the HGC (*pursuant to the provisions of the Ministerial decision under details 79305 ΕΞ 2020, "Enactment of Gaming Regulation on the Suitability of Persons"*) and is decided upon according to specific criteria relevant to their independence, ethic, integrity, prestige, scientific competence, experience and knowledge, whereas, in execution of the aforesaid BoD resolution and the regulatory framework *(HGC decision 554/5/15.04.2021, article 5)* they are assigned to perform at least the following:

- Identify, analyze, and assess the ML/TF risks, in relation to appropriate factors (*such as e.g. the type, frequency, value, methods and means of executed transactions, the countries or geographical areas of players' origin/ destination*).
- Plan and coordinate the policies and procedures to prevent, manage, and mitigate the identified risks and ensure that the extent of the measures taken as the case may be by the Obliged Person is proportionate to the risks of committing ML/TF offences.

- Monitor the applied *(and related to ML/TF)* Corporate policies, procedures, measures and work flows; ensure that these are consistently implemented; assess their efficiency and recommend their re-adjustment and the taking of appropriate corrective actions to the Obliged Person's management and the competent - as the case may be - Corporate bodies, when so required, taking into account the recommendations of the Authority, the HGC, and other competent authorities and bodies (*e.g. the indications as such derive from relevant audit reports*), as well as the developments in the relevant AML/CTF sector.
- Collect and analyze information on the transactions and the Gaming Activity, whenever this activity is under a registered player's profile.
- Establish appropriate channels for the flow of information, the management of complaints, and the receipt of reports forwarded by the Personnel and the Physical Network on unusual or suspicious transactions, as well as on any event that the aforesaid persons are informed of, due to their role, and could be related to AML/CTF matters.
- See to (*inform/ recommend to/ submit a request to, if they deem necessary, the Management or the Company BoD*) the taking and application of the required protection measures (*physical, legal etc.*) by the Obliged Person, both for themselves and their Team, and for information reporting Stakeholders, pursuant to article 26 of the AML/CTF Law.
- Collect, consider, cross-check and assess the information they receive on the conduct or the attempt or the indications on the conduct of Suspicious or Unusual Transactions or Activities, in relation to the corporate policies and keep a relevant record.
- Forthwith inform, on their own initiative, the Authority, when they are aware of or have serious indications about or they suspect that the conducted or attempted transactions, regardless of their value, constitute ML or TF proceeds, by submitting a complete and detailed report. The said obligation also pertains to any case of a Suspicious Transaction attempt. In the case of a report submission, they act as the first point of contact with the Authority, both upon the commencement and during the entire investigation of the case, and respond to all queries and clarifications required, fully cooperating with it. Provided that, following information assessment, the AML Compliance Officer deems that they do not have to proceed to a relevant report, they justifiably close the case.
- Upon their request, they forthwith provide the Authority, the HGC, and other public authorities assigned with AML/CTF duties all required information and details.
- Promptly submit the Compliance Report of article 6 of decision 554/5/15.04.2021 to the HGC and the Board of Directors of the Obliged Person to have appointed them.
- Evaluate, assess, and opine on requests relating to the conclusion of cooperation agreements with members of the Physical Network *(new and/or current)*, which are notified to them by the competent business Units of the Company.
- Assess the compliance of the Physical Network and - where appropriate - recommend the imposition of sanctions by the Compliance Committee and/or the BoD.
- Decide, at his/her discretion, on the refusal to conduct a specific gaming transaction *(in case of any registered palyer's activity)* in cases provided for in the regulatory framework and within the context of applying the appropriate due diligence measures.
- In the case of an application submitted by a Player regarding the granting of a winnings attestation or certificate of article 16 of decision 554/5/15.4/2021, they go through the transactions conducted with the Player that pertain to the period of the attestation or certificate required, and verify that they are not related, directly or indirectly, to ML/CT

actions. In case they have indications to the contrary, they may decide to not grant the winnings attestation or certificate, and to submit a report to the Authority.

- Make recommendations to the competent bodies of the Obliged Person and see to the implementation of personnel and Physical Network Partners education and training programs (*both for those working in the Special AML/CTF Team and those working in other Units of the Company*) on AML/CTF matters. Furthermore, they provide ongoing guidance and address queries submitted by all Stakeholders on AML/CTF matters.
- They are responsible for the communication of the Obliged Person with the HGC, the Authority, and other co-competent authorities on matters that fall under their competence.
- Cooperate with and share information with the Coordinating AML Compliance Officer and the AML Compliance Officers of the other Group Obliged Persons.

Respectively, the Board of Directors of the parent company OPAP S.A. has appointed a Group AML Compliance Coordinator, having as his/her main mission to coordinate the activities of the AML Compliance Officers of all Group Obliged Persons in Greece, active in the Gaming sector, and share *(with the AML Compliance Officers)* relevant information, where so required. Consequently, the Coordinator may, at his/her own discretion, contact and share views/ information with the AML Compliance Officer of Hellenic Lotteries S.A.

2.3. Personnel of Other Company Units and Physical Network Partners

As is the case with all types of risk relating to the nature of the Company's activities, in this case as well, it is not possible to have a sufficiently effective AML/CTF risk management unless all Stakeholders (*mainly the Personnel and the Partners of the Physical Network*) recognize the significance of their role and constantly operate in full alignment with the Company's pursuits and efforts to eradicate ML/TF risk.

Therefore, both the Personnel (*with the emphasis placed on those involved in Company activities that relate to the conclusion of relationships with Physical Network Partners, to sales and, in general, to the processing of customer transactions, to the support of the aforementioned activities, as well as to those having access to details/ files/ systems affecting their AML/CTF activities*) and the Company's Physical Network Partners at least apply the following:

- Peruse, comprehend, and apply the present Policy and all due diligence measures described herein, focusing on the procedures/ guidelines regarding the authentication and verification of customers' *(KYC – Know Your Customer)* and Physical Network Partners' identity *(KYP - Know Your Partner)* and the investigation/ documentation procedures regarding their transactions *(KYT – Know Your Transactions)*, when and where so required.
- See that the electronic and physical Customer/Partner databases of the Company *(e.g. winning certificates platform, agents registry)* are updated with sufficient, in terms of quality and quantity, information on every new or existing Customer/Partner.
- Stay constantly alert for the identification of suspicious or unusual transactions and customer behaviors, in accordance with the existing typology *(both the one set forth in general by the institutional framework, e.g. BCC 285, and the one specified by the Company)* or their personal opinion/ assessment, and submit relevant internal reports *(using special corporate forms and communication channels to this end)* to the Company's AML Compliance Officer.

- Participate in all relevant training activities to which they are invited, and fully complete the said obligations of theirs.
- Never disclose any information brought to their attention regarding investigations conducted on involved customers or Physical Network Partners or any third party related thereto or any internal reports that are carried out or will be carried out thereon *(Tipping Off)*.
- Forthwith address the requests presented by the Company's competent Executives, the AML Compliance Officer or other control bodies thereof *(e.g. Internal Audit Unit)* for the provision of written, oral or other information on customers, partners and their transactions.

At the same time, the human resources of other competent Units on the IT/ organizational infrastructure of the Company and the Group (*e.g. Technology & Digital Team, Information Security Team*) and the management of the relationship with the supervisory Authorities (*Legal, Regulatory and Compliance Team*) contribute to the implementation of the provisions of the present Policy as follows:

- They cooperate with, participate in, and support the development of IT systems, which are required for the actual implementation of the Policy.
- They ensure the highest possible security level of information that is entered and subject to processing by the said IT systems.
- They participate, if such a need arises, by opining/ consulting and/or tangibly contributing to the drafting and issuance of any systems' user manuals, policies/ procedures, of informational material and any other material relevant to AML/CTF risks.
- Suggest any kind of improvements regarding the above-mentioned and all other issues that pertain to the Company's infrastructure for the prevention and suppression of ML/FT.

2.4. Internal Audit Unit

The Group Internal Audit Unit, being the suppressive pillar of the Company's Internal Control System, incorporates the present Policy and the internal processes deriving from it in its annual audit plan. In addition, it evaluates the adequacy and efficiency of the measures taken by the Company, in order for the ML/FT risk to be identified, assessed, monitored and managed.

3. Management of Customer and Physical Network Partners – Adoption of Infrastructure and Taking of Measures for the Mitigation of ML/TF Risk

3.1 Criteria and Conditions for the Acceptance of Customers/ Partners for the Conclusion of Business Relationships and the Conduct of Single Gaming Transactions

The Company has set forth specific criteria, which - if confirmed to stand - constitute a strong basis to decline the conclusion of new Business Relationships, to terminate and/or to freeze current ones, as well as to decline single transactions of Customers. Specifically:

Customers/ Players

The Company, given the nature of the services already offered *(lotteries, skratch)* in combination with the fact that they are offered exclusively through its Physical Network of Partners where the participation is anonymous *(except for betting cases of a value higher than €2,000)*, does not enter into Business Relations with customers. Instead, it executes their individual / occasional transactions *(participation in bets, redemption of winnings, granting of winning certificates)*, apart from the cases where it is established that the respective potential customer:

- Is a minor (*i.e. younger than 18*), pursuing any gaming activity.
- Is a legal person or entity, meaning they are not a natural person.
- Does not promptly present, in cases clearly provided for in the respective regulations, the necessary information and sufficient/ appropriate documents to the Company in order to render feasible both the authentication and verification of his identity, and the application of the necessary due diligence measures, required by the framework. Provides false information or information that contradicts existing information and/or cannot be reliably cross-checked.
- In the case of games of chance, which are offered via the Company's Physical Network, he/she tries to carry out a transaction/ wager remotely (*e.g. over the phone*) or via interposed persons and not by being physically present.
- Happens to be included in a sanction list of persons for whom restrictive measures apply, pursuant to decisions taken by the European Council and/or of the UN Security Council and/or OFAC *(Office of Foreign Assets Control).*
- Is included in a list of persons with whom the Company has previously decided to terminate a Business Relationship maintained therewith *(e.g. for reasons that pertain to the attempt to commit fraud or to the existence of strong indications of an overall unlawful conduct or activity, which constitutes suspicious ML/CT activity)*.

Physical Network Partners

The Company does not conclude Business Relationships or extends current ones in case it is confirmed that:

- Any potential Partner of the Physical Network does not promptly present the necessary information and sufficient/ appropriate documents to the Company (*or deliberately*

presents false/ misleading information) in order to render the authentication and verification of the owner's *(in the case of a partner being a natural person)* and/or the ultimate beneficial owner's identity (*e.g. in the case of a legal person*) feasible, as well as the application of the all due diligence measures required by the framework.

- The Owner or the Ultimate Beneficial Owner or other significant persons *(e.g. Agency Manager)* employed in the Physical Network happen to be included in a sanction list to which prohibitive measures apply pursuant to decisions of the Council of the European Union and/or of the UN Security Council and/or OFAC *(Office of Foreign Assets Control).*
- The Owner or Ultimate Beneficial Owner of a member of the Physical Network is included in a list of persons on whom the Company has previously decided to terminate any Business Relationship maintained therewith (*e.g. for reasons that pertain to the attempt to commit fraud or to the existence of strong indications of an overall unlawful conduct or activity, which constitutes suspicious ML/CT activity*). In this case, any requests may be accepted, on the sole condition of the approval provided by the Compliance Committee to which a relevant justified recommendation must be presented on behalf of the competent business Units of the Company, which will be taking into account the background of the requesting party, based on which their Business Relationship with the Company had been terminated/ had not been extended, and will be explaining the reasons for which it is estimated that the Company must conclude anew/ extend the Business Relationship therewith.
- During the initial assessment of a new request, the requesting party is allegedly directly or indirectly involved, in accordance with information coming from reliable sources or it is known that they are involved and/or have been convicted for committing primary offences of article 4 of L. 4557/2018 (*e.g. drug trafficking, terrorism, organized crime*).

3.2 Establishment and Continuance of Business Relationships - Application of Due Diligence Measures

3.2.1 Applied Due Diligence Procedure

In its effort to identify unusual/ suspicious transactions and activities of entities with which it concludes Business Relationships *(e.g. with Physical Network Partners)* and generally of the entities that use its services *(e.g. Players)* so as to deter the risk of using it for ML/TF reasons, the Company takes a series of measures and performs various tasks, which (measures and tasks) are overall set forth as "Due Diligence Procedure".

The procedure and the necessary, as the case may be, Due Diligence measures are implemented by the Company prior to the establishment of any Business Relationship or the execution of any transactions relevant thereto, as well as during finalized Business Relationships (*whenever deemed necessary*), whereas they are scaled depending on the quantity and quality of the information required to be collected and processed (*all 3 types are analyzed as follows*):

- Simplified Due Diligence (*hereinafter **"SDD"***)
- Usual Due Diligence (*hereinafter **"UDD"***)
- Enhanced Due Diligence (*hereinafter **"EDD"***)

In this context, it is stated that the main component and condition regarding the sufficiency of the applied Due Diligence Procedure by the Company and the application of the respective measures pertains to knowing each customer/ Player *(wherever required)* and Partner of the Physical Network with whom the Company establishes a business relationship *(KYC - Know Your Customer & KYP – Know Your Partner)* and the transactions/ activities that they conduct *(KYT – Know Your Transaction)*.

In particular, this knowledge *(KYC & KYT)* about the customer/ Player consists in the collection of reliable/ objective, personal, demographic, financial and transactional data/ information regarding the customer, and respectively targeted information and documents on the Physical Network Partner (*KYP*), which *(data and information)* is used for the authentication and verification of their identity. At the same time, it is assessed by drafting and determining their complete profile, including their reasonable and anticipated behavior, which in turn constitute the main point of reference when trying to identify suspicious and/or unusual transactions/ activities and, in general, any deviating transactional behavior of theirs.

Therefore, regarding any Business Relationship, as well as any Player transaction exceeding the thresholds set forth by the Regulation, the Company sees to the proportionate and gradual implementation/ ensuring of specific measures/ conditions, which *(measures and conditions)* are mentioned in detail in the following sub-chapters on the Usual and Enhanced Due Diligence measures.

3.2.2 Criteria and Conditions of Application of the Due Diligence Procedure

The Company implements the Due Diligence Measures on the condition that any of the following cases applies to the customer/ Player, the Physical Network Partner and their transactions:

- When a Business Relationship with a Physical Network partner is about to be concluded.
- When, with regard to the Physical Network, a 2.000 EUR and more transaction is carried out by a Player, during the Participation in a Game of Chance or the collection of winnings, regardless of whether the transaction is carried out in one single act or more, which seem to be connected The aforesaid thresholds are calculated at a gaming day level, which in turn is calculated based on the working hours of the Physical Network within a calendar day.
- During the issuance of a payment order to the Bank for winnings generated from games of chance, which are offered by the Physical Network and pursuant to the thresholds laid down in the HGC decision 554/5/15.4.2021 *(optionally for gross revenues of €1.000-2.000 per slip and mandatorily for revenues of >€2.000 per slip)*.
- During the issuance of a Winnings Attestation or Certificate for taxation purposes.
- When there is an ML/TF suspicion, regardless of any deviation, exception or minimum threshold laid down in the legal and regulatory framework.
- When doubts are raised on the accuracy or sufficiency of the data provided and collected for the verification of the customer's identity.

3.2.3 Application of Simplified Due Diligence (*SDD*)

SDD is the lowest level of Due Diligence, which may be applied to a customer/ Player (*the Company does not apply it in the case of conclusion of Business Relationships with Partners of the Physical Network*) and has a potential application to cases, where the ML/TF risk is extremely limited either due to the kind/ type of the customer/ transacting party or due to the nature of each transaction executed by them or the product/ service provided to them or due to other reasons, which contribute to the radical mitigation of the aforesaid risk.

The Company applies SDD measures only following an HGC approval to a request it has submitted to the said supervisory authority pertaining to the exemption of specific Games of Chance and/or categories thereof from specific or all the Regulation requirements.

3.2.4 Application of Usual Due Diligence (*UDD*)

UDD is the minimum level of Due Diligence that the Company has to apply to the Business Relationships it concludes and maintains with Partners of its Physical Network, as well as to the Players' occasional transactions *(during a betting transaction higher than €2.000, the collection of winnings via Banks, the granting of a winning certificate)*:

Case of Application A	Case of Application B	Case of Application C
Granting of a Winning Certificate to an applicant player	Passing-by customer of Physical Network, who executes **a transaction of > €2.000**.	**Conclusion of a Business Relationship with a Partner of the** Physical Network

Under the aforesaid specific conditions, which require the application of UDD measures, the Company requirements with regard to the Player include the following (*it is noted that the following are not always applied in their entirety in the case of Players, who simply carry out occasional transactions of >€2.000 via the Physical Network, e.g. it is not feasible to readily prepare the financial/ transactional profile for the said Players*):

- The authentication and verification of the Player's identity on the time set forth in the Regulation, based on evidentiary documents, data or details from reliable and independent sources at the time and in the manner specified in the Regulation.
- At a time which is feasible, the control of the Player's identity as to whether they are nationals of a country, which has been characterized as high-risk for ML/TF by the European Commission or belongs to Non-Cooperative Jurisdictions or included in respective lists of the Authority, of the competent police, administrative, and judiciary authorities, where those lists exist and are accessible to the Company, as well as in the HGC registers relating to restrictive measures.
- At a time which is feasible, the control of the Player's identity and the confirmation that they are not a Politically Exposed Person or a Person listed in international sanction lists *(EU, UN, OFAC)*.
- The ensuring that the payment of winnings, which exceed the thresholds set forth as the case may be in the Regulation are only carried out via the Payment Services Providers, following the authentication and verification of the Player's identity, as well as the Player's verification as the beneficiary of the relevant payments account.

- The issuance of a winnings' attestation or certificate, under the terms and procedures set forth in the Regulation.
- The decline to provide services *(conclusion/ continuance of a Business Relationship or the conduct of a transaction)*, to pay winnings, to issue a winnings attestation or certificate in case the Player's identity authentication and verification conditions have not been met, as well as in case they know or have serious indications or suspect that the Player aims - based on their Gaming Activity - at legalizing proceeds generated from criminal activities or the financing of terrorism.

As to the application of UDD measures by the Company during the conclusion of Business Relationships with Partners of the Physical Network, those include the first 3 respective measures, which are also applied in the case of a Player, highlighting that the provisions on Politically Exposed Persons are not applied in the case of a Partner. It is clarified that the application of the said measures in the case of Partners of the Physical Network, who are legal persons and/or other legal arrangements/ entities focuses on the ultimate beneficial owner(s) of the said entities.

Moreover, with regard to Partners, their compliance with the provisions of the Policy and the Regulation in general is regularly monitored, and where so required, the Company takes appropriate measures aiming at achieving its alignment with the provisions of the legal-regulatory framework.

3.2.5 Application of Enhanced Due Diligence (*EDD*)

In case where the Company deems that there is an increased ML/FT risk, it takes EDD measures, i.e. it implements all the provisions described in chapter 3.2.4 of the present Policy, regularly reassessing the involved entities and the Business Relationship, which is relevant thereto.

Indicatively, the Company applies EDD measures, in the following cases:

- When it knows or has indications, information or evidence that a Suspicious or Unusual Transaction is conducted or attempted.
- When it knows or has indications, information or evidence on any of the following:
  - The Player Participates in Games of Chance as an interposed person as per the meaning of par. 6, article 32 of L. 4002/2011.
  - The Player has used or attempts to use Means of Payment that belong to third parties.
- When it ascertains that the Player is national to a country, which has been characterized as an ML/TF high-risk country by the European Commission or belongs to Non-Cooperative Jurisdictions.
- When it ascertains that the Player is listed in the non-licensed providers list of par. 7, article 48 of L. 4002/2011 *(A 180)*.
- When the winnings to be paid exceed the amount of 50.000 EUR.

Under the aforementioned conditions, which require the application of EDD measures, the Company requirements as to the Player indicatively include, apart from the provisions of sub-chapter 3.2.4, one or more of the following measures:

- The collection of additional information and documents from the Player in relation to their identity and the source of the funds that they use to wager.
- The requirement for physical presence in the Company's premises *(e.g. in the case of payment of high winnings)*.
- Communication with the Greek Financial Intelligence Unit or other competent pursuant to the law Authorities *(at the discretion of the AML Compliance Officer)*.
- Communication with AML Compliance Officers or competent Executives of other Obliged Persons, as such are laid down in the Law against ML/TF.
- Decline to provide services *(conclusion/ continuance of a Business Relationship or execution of every transaction)* - the said measure is repeated despite the fact that is also stated in the case of UDD measures for reasons pertaining to a greater chance of it being implemented in cases such as the aforementioned.

3.3 Termination of Business Relationships

The Company considers the termination of the established Business Relationships in the following cases:

- When it is confirmed that a criterion(a) or conditions on the non-acceptance, as such are mentioned in chapter 3.1 of the present, apply to a current Business Relationship. More specifically, when one and/or more cases out of those provided for in sub-chapter 3.1 happen to be noticed following the conclusion of a Business Relationship with the Partner of the Physical Network *(indicatively, due to the change in their details or due to the fact that during the relationship it is ascertained that they systematically breach the present Policy and/or other Policies and Regulations of the Company or due to the fact that reports have been repeatedly submitted on them to the Greek Financial Intelligence Unit or due to the imposition of asset freezing measures by the competent Authorities)*, the Company takes all necessary actions and pursues as the case may be the interruption and/or freezing of the relevant Business Relationships *(see sub-chapter 3.3)*. In some cases, the said interruption and/or freezing takes place immediately *(e.g. if a Partner of the Physical Network is included in sanction lists)*, whereas in some other cases, the Company's Board of Directors acts upon the said matter, following a recommendation made by the Compliance Committee, which has been previously notified by the AML Compliance Officer and other involved persons.
- In case the counter party to the Business Relationship has been repeatedly reported to the Greek Financial Intelligence Unit, without a change being noticed in their behavior and given that no special relevant instructions have been received by the said Authority.

4. Reporting of Suspicious Transactions

Pursuant to the Law against ML/TF, the Regulation and the provisions of sub-chapter 2.2 of the present Policy, the AML Compliance Officer is obliged to forthwith inform, on their own initiative, the Authority, when they are aware of or have serious indications on or suspect that the transactions conducted or attempted, regardless of their value, constitute proceeds generated from ML or TF, by submitting a complete and detailed report.

The identification of the aforesaid cases and the respective briefing provided to the AML Compliance Officer on an unusual and/or suspicious transaction/ activity may arise either via the central IT infrastructure and procedures developed by the Company to this end or if any Company Officer or Physical Network Partner notices such event and reports it *(to the AML Compliance Officer and their team)*, during the performance of their role and tasks. As to the second case, the Stakeholders may contact the AML Compliance Officer and their Team using different means, such as:

- Via a direct personal contact/ meeting or phone communication.
- Anonymously and/or not through the mailbox WBAML@opap.gr. Only the Group AML Compliance Coordinator, the AML Compliance Officer and certain members of their Team have access to the said email account.

It is noted that the Company evaluates different factors and features to assess a transaction/ activity as unusual and/or suspicious, including the Indicative typology of suspicious or unusual transactions, which is included in Annex III of the HGC Regulation.

5. Tipping Off and Protection of Reporting Persons

5.1. Tipping off

Any Stakeholder (*Company Personnel, Physical Network Members etc.*) and third party that is well placed to know due to their relationship with the Company is prohibited from transferring/ disclosing *(Tipping Off)* to involved Players/ Physical Network Partners/ other entities *(or any other third party related or not to them)*:

- Information they become aware of in connection with investigations having been conducted, are being conducted or are to be conducted on them *(the involved Player etc.)* with regard to ML/TF offences.
- Details having been transferred, being transferred or about to be transferred in connection with ML/TF offences.
- Suspicious Transactions Reports on them having been submitted, being submitted or about to be submitted to the Greek Financial Intelligence Unit in connection with ML/TF offences.

Additionally, in any case where the Company decides to decline the execution of a gaming transaction or the interruption of a Business Relationship, it uses any suitable means to not disclose to the involved person that the reason for this transaction decline or the interruption of the Relationship is that they know or have serious indications about or suspect that Suspicious or Unusual Transactions have been conducted or attempted.

It is noted that if any of the Company's Employees/ Executives breaches this particular prohibition, they must anticipate the imposition of respective, commensurate, as the case may be, disciplinary sanctions *(possibly including the termination of their employment relationship with the Company),* whereas at the same time, given that such act also constitutes a breach of the applicable legislation, the said person may suffer additional legal consequences *(criminal liability).*

5.2. Protection of Reporting Persons

The Company hereby acknowledges and sets forth that the Reporting Persons, i.e. the AML Compliance Officer along with their specialized operational Team falling under them, the rest of the Company personnel and its Physical Network Partners that may participate in any - within the context of the activities to face the ML/TF risk - bona fide information exchange within the Company and the Group thereof, as well as in the bona fide disclosure of information and submission of suspicious transactions reports to the Greek Financial Intelligence Unit and all other competent as the case may be Supervisory and Public Authorities, are in no way liable against eventual claims raised by the subject of the aforementioned disclosures/ reporting on the grounds of the breach of a legislative, regulatory, administrative or contractual prohibition to disclose information or any other breach whatsoever.

The Company as a whole, its Management, the members of its Personnel and its Physical Network see to and proceed to all actions in order to maintain the anonymity of the AML Compliance Officer and any other person participating in the collection of information, as well as in the drafting and reporting on suspicious and/or unusual transactions to the competent Supervisory and Public Authorities. Therefore, by virtue of the present Policy, the provision/ disclosure of any personal or other details of the aforesaid persons to third parties is prohibited, with the exception of Supervisory and/or Public Authorities. A breach of the said prohibition may lead to the imposition of relevant, commensurate, as the case may be, disciplinary sanctions to the breaching parties.

At the same time, pursuant to its obligations under article 26 of the Law against ML/TF, in the aforementioned cases of bona fide disclosure of information and submission of suspicious transactions reports to the Greek Financial Intelligence Unit and all other competent authorities, even if it is finally proved that no criminal activity has been undertaken by the said persons, the Company undertakes to not use the said fact as a reason to terminate the employment agreement of the Reporting Persons or to worsen the terms of the said agreement. The Company will instead provide the overall required physical, legal, and any other kind of cover and security to the Reporting Persons to protect them against revenge, intimidation, threats, retaliation, hostile actions, negative discrimination and any other kind of negative development and conduct.

6. Training

Being an Obliged Person, and depending on the – from time to time – risks under assessment, their nature and size, the Company adopts sufficient measures so that the Personnel and the Members of its Physical Network become acquainted with the provisions of the legal and regulatory framework on AML/CTF in force, they act efficiently during their participation in activities, which entail ML/TF risks, and they handle any relevant incidents that they become aware of, in the best possible manner.

In this context, the AML Compliance Officer, in cooperation with the Group's Human Resources Team, the Retail Network Training Team, and all other involved Services carry out all necessary actions for the internal preparation, regular update and attendance *(by appropriate/ targeted audience)* of training programs on AML/CFT. The said training programs

cover as a minimum the relevant legislation and the Regulation, the obligations arising therefrom on Obliged Persons, the personnel and their Physical Network, the Corporate Policy in force and the adopted procedures relevant thereto, whereas they adapt to the audience they address.

In all cases, the competent Units monitor the participation in the aforementioned training programs and necessarily keep relevant successful attendance records, which they present to auditing and other Authorities, if such a need arises.

7. Record-Keeping

The Company sees to the keeping/ safekeeping of a sufficient documents and information record, pursuant to the legal requirements on ML/TF and the Regulation.

All relevant Company files are kept for a period of at least five (5) years as from the expiration of each Business Relationship or the execution of each single transaction, unless their keeping is permitted or imposed for a longer period under a different legal provision or regulatory decision.

The keeping of records is carried out in an electronic (*mainly*) format, in a way that allows for their easy recovery and access thereto, if so required. In case the keeping of a file in soft copy is not possible *(e.g. contractual documents with Partners of the Physical Network)*, all necessary measures are taken for the keeping of physical documents. These documents are kept according to the method that also applies to soft copy documents.

Both the IT systems of the Company and the policies and procedures applied to the keeping of physical files *(where necessary)* are arranged in a way that ensures the protection of confidentiality and, in general, the provisions of the legislation in force on the protection of personal data. This fact is subject to preventive and regular control by the Company's competent control bodies and the AML Compliance Officer who have to report any case of breach and suggest and/or impose the taking of necessary measures.

8. Reports

The Company is obliged to draft a semi-annual and annual regular report on its compliance with AML/CFT provisions.

The report content is set forth in article 6 of the Regulation.

The report is drafted by the AML Compliance Officer and submitted to the Company Board of Directors. Having been informed and assessed the content of the report, the Board of Directors or a member authorized by it from time to time in turn drafts a relevant memo, including their opinion on those stated in the report. Both the report and the BoD opinions are submitted to the HGC, pursuant to the dates set forth in the Regulation.

Additionally, by 31st January of each year, the Company submits to the HGC:

- For games of chance offered via the internet or require an Individual Player Card (IPC), the same account and the Players' account they keep with PSPs, as well as the Means of Payment they accept for the deposit of the Participation amounts and the payment of winnings to Players.

- For games of chance offered via the Physical Network, the accounts they keep with PSPs and the Means of Payment, which they use and accept for the deposit of the Participation amounts and the payment of winnings to Players.

Revision History

Version	Date	Owner	Comments/ Main Changes
1	30/7/2019	A. Panagiotou	*In replacement of the previous version dated 23/4/2015*
2	07/04/2022	D. Papakonstantinou	*Adjustment to the new Regulatory Framework (HGC Decision no. 554/5/15.4.2021) In replacement of the previous version dated 30/7/2019*

Document Approvals

	Full Name	Title
Owner	D. Papakonstantinou	AML & Antifraud Manager
Reviewed & Approved	A. Panagiotou	Treasury, Credit Risk & AML Director
Reviewed & Approved	Pavel Mucha	CFO
Approved	BoD	Meeting 08/09/21 (item 6.1)