



Tipico Group AML/CFT Policy

Contents

1.	INTRODUCTION	3
2.	GOVERNANCE AND RESPONSIBILITIES	4
3.	AML/CFT FRAMEWORK AND CONTROLS	5
4.	CUSTOMER ACCEPTANCE AND CUSTOMER DUE DILIGENCE	6
5.	HIGH RISK SCENARIOS	7
5.1	POLITICALLY EXPOSED PERSONS	7
5.2	SANCTIONS	8
5.3	MEASURES IN CASE OF PEP AND SANCTION MATCHES	8
6.	SUSPICIOUS TRANSACTION/ACTIVITY REPORTING (STR/SAR)	9
7.	RELIABILITY OF STAFF	10
8.	AML/CFT TRAINING PROGRAM	10
9.	RECORD KEEPING	10

1. INTRODUCTION

Tipico as one of the leading gaming providers commits itself to the highest standards in protecting its business of misuse by Money Laundering (ML) and Funding of Terrorism (FT) or any other criminal activities.

Tipico holds, amongst others, licenses for the operation of sports betting and online casino games granted by the Malta Gaming Authority (MGA) and is therefore considered a subject person under Maltese AML/CFT legislation, namely the Prevention of Money Laundering Act (PMLA), the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR). The requirements of the Maltese legislation apply to Tipico group-wide. Local Tipico Group companies may have additional local policies and procedures designed to comply with their local legislation, regulations and any government approved guidance in the jurisdiction(s) in which they operate.

The key objective of this policy is to set the structure to prevent that Tipico's services are being misused as a channel for ML, FT or fraudulent activities and that these services comply with the applicable Anti-Money Laundering (AML) and Counter Funding of Terrorism (CFT) rules and regulations which are set in the EU AML Directives, especially in the 4th and 5th EU-AML directive (2015/849 and 2018/843), and their transposition into national law in Malta, Germany and further jurisdictions as applicable. This is to protect all Tipico entities and employees from being involved in illegal activities and provide them with clear guidance.

This policy is applicable to all employees belonging to the Tipico Group (hereinafter the "Tipico Group", the "Group" or "Tipico") and will be reviewed annually and revised as needed.

Tipico Group entities are subject persons to the applicable laws and regulations and will adhere to them in every country where Tipico is conducting business in or with.

The Maltese legislation, together with regulations, rules and industry guidance such as the Financial Intelligence Analysis Unit's FIAU Implementing Procedures Part I and II (for the Remote Gaming Sector), form the cornerstone of AML/CFT obligations for subject persons and outlines the offences and penalties for failing to comply.

The Board of Directors and all group employees are required to protect Tipico and its reputation by complying with these standards from being misused for ML, FT or other misconduct.

All measures are to be applied on a risk-based approach. The risk-based approach allows Tipico, within the framework of the legal requirements, to adopt a more flexible set of measures, in order to target resources more effectively and apply preventive measures, that are commensurate to the nature of risks – to be able to focus our efforts in the most effective way.

By following the risk-based approach, risks in different areas can be identified and measures to mitigate these risks can be applied according to the level of all risks identified. These measures then will be implemented to reflect the day-to-day responsibilities under applicable AML/CFT regulations.

Tipico has a zero-tolerance policy for ML, FT or any other financial crime activities.

2. GOVERNANCE AND RESPONSIBILITIES

The Board of Directors has appointed the AML Officer to act as **Money Laundering Reporting Officer** (MLRO). In order to fulfill his tasks, the MLRO has the right to access all necessary data, documentation and information.

The MLRO is reporting directly to the responsible member of the Board of Directors, the Chief Regulatory Officer (CRO) and provides the CRO with regulatory updates, updates on on-going projects and relevant KPIs on a monthly basis.

Tipico has appointed the AML Compliance Manager to act as designated employee (Deputy MLRO) to assist and, whenever necessary, temporarily replace the MLRO when absent.

Each Tipico Group entity that is a subject person and an obliged entity under AML/CFT laws and regulations shall appoint a responsible MLRO.

The AML Officer shall be responsible for the administration, revision, interpretation and implementation of applicable laws and regulations as fundament to this policy.

This policy establishes the framework for adequate AML/CFT procedures, AML/CFT trainings and AML/CFT controls, which need to be applied in all business units based on a risk-based approach in order to manage the ML and FT risks of the Tipico Group appropriately.

The AML/CFT program is directed by the AML Officer and it is designed to address also related risks in financial crimes and to provide unobscured guidelines for all employees when it comes to prevent financial crimes such as ML and FT.

Within the Group, responsibilities are assigned to designated teams and employees, which support the MLRO in his duties, in order to secure the implementation and the following of Tipico's policies and procedures. It is the MLRO's responsibility to ensure that operational procedures are updated on a regular basis, at least once a year, and will be approved by himself in cooperation with the responsible team leaders/managers.

3. AML/CFT FRAMEWORK AND CONTROLS

By following the risk-based approach, all possible risk areas and risks can be identified, and mitigating measures are applied according to the grade of risks that have been assessed. These measures will then be implemented to reflect the day-to-day responsibilities under applicable AML regulations.

A **business risk assessment** and a **customer risk assessment** are performed. Tipico implements an ongoing corporate AML/CFT risk assessment to analyse the level of risk that its customers, services, channels, products or geographic locations of its legal entities are posing. The results of the risk assessment lead to appropriate risk mitigating actions.

Tipico Group has set out its comprehensive set of risk mitigating measures in its IT-based AML/CFT Framework of risk assessment, policies, procedures, trainings and controls.

Constant safeguarding of AML/CFT compliance is achieved by designing and installing also controls to manage and reduce the impact of identified risks and to assess the effectiveness and functionality of taken measures.

On an ongoing basis, the MLRO will monitor the AML/CFT controls to improve their efficiency, proper records of taken actions and the reasoning behind such actions are kept and documented.

4. CUSTOMER ACCEPTANCE AND CUSTOMER DUE DILIGENCE

Tipico has adopted a **Customer Acceptance Policy** in conformity with its obligations as licensed gaming operator to meet all applicable legal requirements such as requirements regarding responsible gaming, player protection and anti-financial crimes. The said policy is not only used for AML/CFT purposes, but also player protection, and is maintained in a separate document.

The Board of Directors and senior management of Tipico have established a strong player protection and AML/CFT culture and are constantly communicating a clear message to all employees that the company as a good citizen protects minors and its customers.

Tipico adopted a zero-tolerance approach to financial crime or any other illegal activities to prevent the company from being misused for unlawful purposes. Tipico will not tolerate money laundering or funding of terrorism at whatever level, and will not knowingly conduct business with individuals or entities it believes to be engaged in such activities.

Depending on the risk arising from a customer, different levels of customer due diligence (CDD) need to be applied, distinguishing between simplified due diligence (SDD), standard customer due diligence (CDD) and enhanced due diligence (EDD).

Group-wide any natural person or corporate entity as business partner shall be identified adequately by full registration of personal/company data, be risk rated and monitored according to the documented processes (procedures) in place.

Personal data such as the official full name, place and date of birth, permanent residential address, identity reference number, where available and nationality should be complemented with information and documentation on the source of wealth/funds as well as any other information obtained by the customer on a risk-based level of CDD. The nature and extent of CDD will depend on the risk presented by the customer, franchise partner or supplier.

The CDD measures also include, besides identifying the customer or business partner, the verification of said customers/business partners based on permissible documentary or electronic sources as well as the identification and documentation of its Ultimate Beneficial Owners (UBOs) and legal representatives where applicable.

No natural person is to be conduct business with, if said person does not meet the legal requirements or is prohibited or excluded to use our services for any reasons. No anonymous or fictitious named accounts can be opened or obtained. Not more than one active customer account shall be allowed per customer.

Generally, no business can be carried out with any natural person or corporate entity if that subject is suspected to be or confirmedly involved in any relevant illegal activities, especially related to ML, FT or fraudulent behaviours.

In cases of doubt the MLRO must be involved for a risk assessment and initiating appropriate risk mitigating measures if applicable.

5. MONITORING & SCREENING ACTIVITIES

Tipico enforces its efforts to establish and maintain industry-leading procedures and systems to monitor customer behaviour and activities risk-based and on an ongoing basis to ensure the detection of any unusual behaviour or transactions.

Applicable laws on the prevention of ML and FT require Tipico as a licensed gaming company to determine if customers or business partners are Politically Exposed Persons (PEPs) or subject to local or international sanctions.

PEP and sanctions screenings are conducted at the beginning of the customer relationship and going forward on an ongoing basis. PEP/Sanction checks are also carried out manually during EDD investigations, if a customer has been identified as a potential high risk customer.

5.1 Politically Exposed Persons

The requirements relating to PEPs are of a preventive and not criminal nature by law. Tipico has an appropriate risk management system in place, including risk-based procedures, to determine

- whether a customer or the management or the beneficial owner of a business partner is a politically exposed person,
- whether this person can be accepted as a customer and
- which mitigating measures need to be applied.

Generally, a person is politically exposed if he/she holds or has held a prominent public function in the past 12 months. Such prominent public functions shall include, but are not limited to:

- Heads of State,
- Heads of Government,
- Ministers and Deputy and Assistant Ministers and Parliamentary Secretaries;
- Members of Parliament;
- Members of the governing bodies of political parties;
- Members of the Courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
- Members of courts of auditors, Audit Committees or of the boards of central banks;
- Ambassadors, charge d'affaires/diplomats and other high-ranking officers in the armed forces;
- Members of the administration, management or boards of state-owned corporations; and
- anyone exercising a function equivalent to those set out in paragraphs (a)-(f) above within an institution of the European Union or any other international body.

Close family members, such as

- the spouse or any person considered to be the equivalent to a spouse,
- parents and children and their spouses or any person considered to be the equivalent to a spouse are to be classified as PEPs as well.

This also applies to persons who are considered "known to be close associates". This definition applies to every natural person who has joint profits from assets or established business relationship or any other

close business relations with a politically exposed person and also natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

5.2 Sanctions

Tipico is required to screen customers and on a risk-based level also business partners against sanctions lists issued, among others, by the United Nations, European Union and US Office of Foreign Assets Control (OFAC) at a minimum in all jurisdictions in which Tipico Group operates, unless to do so would conflict with local legislation.

Whereas Tipico can decide whether to accept PEPs as customers, under no circumstances can business be carried out with any sanctioned natural person or corporate entity.

5.3 Measures in case of PEP and sanction matches

Tipicos relevant operational teams have procedures in place, which describe how to deal with PEP/sanction alerts, identify alerts as false positives or true matches and escalate true matches to the MLRO and Deputy.

The MLRO and the Deputy have a separate procedure in place, which defines the steps that need to be taken if the designated teams escalate a PEP or sanction match.

According to the escalation procedure,

- senior management approval for the establishment or continuation of a business relationship with a PEP has to be obtained;
- EDD measures, including establishment of the source of wealth and if applicable the source of funds that are involved in such business relationships, need to be applied
- enhanced, ongoing monitoring of those business relationships needs to be applied.

If a customer is identified as a sanctioned person, the following actions are mandatory:

- immediately freeze all assets held on behalf of the sanctioned person and
- inform the Sanctions Monitoring Board (SMB) to receive further instructions.

6. SUSPICIOUS TRANSACTION/ACTIVITY REPORTING (STR/SAR)

Suspicious activities and/or transactions must be identified, handled, escalated and reported promptly.

Tipico employees who identify/detect unusual or suspicious activities and/or transactions are obliged to report these incidents to the MLRO immediately. Tipico employees can use different ways to submit internal SAR/STRs and are instructed accordingly.

Once an internal report is received, the MLRO and his assignees will investigate the customer's account to assess the unusual behaviour and/or suspicion described within the internal report. Based on the outcome of the investigation, the MLRO will decide whether to report the suspicion externally to the relevant authorities or to close the internal report with documented reasons.

Detailed procedures are available for all the departments involved in internal/external reporting on how to investigate internal reports, how to submit reports externally and which risk mitigating measures to take.

The suspected/involved customer or any other third party is not to be alerted of any investigations or reports regarding ML/FT, as under no circumstances a "Tipping-off" is accepted or tolerated, given the fact that this would be a serious criminal offence.

The MLRO is obliged to report any suspicious activity or transaction to the respective authorities where the MLRO knows, suspects or has reasonable grounds to suspect ML/FT promptly. The internal or external reporting of a suspicious activity cannot be suppressed.

7. RELIABILITY OF STAFF

Tipico ensures the review of employees for their reliability with qualified measures, through employee control and appraisal systems during the hiring process and on an ongoing basis during the time of employment by management evaluation.

8. AML/CFT TRAINING PROGRAM

Adequately AML/ CFT trained staff is a cornerstone of every effective AML/CFT program to protect the company of related risks. It creates also the level of awareness that is key to report any suspicious activity without undue delay.

New employees shall receive anti-money laundering training as part of the mandatory new joiners training program (as applicable in their respective company).

All employees are required to complete a web-based AML/CFT training annually. Employees with operational or other substantial AML responsibilities shall receive additional AML/CFT trainings as applicable, especially if they are responsible for the maintenance of customer relationships or for processing transactions.

9. RECORD KEEPING

All identification documentation and service records shall be kept for a minimum period of no less than five years after the termination of the contractual relationship with the customer notwithstanding retention periods of other laws as e.g. tax or data protection laws.

AML/CFT relevant data in relation to internal investigations, KYC measures or STRs/SARs shall be obtained for five years and - if no further need is identified - deleted after.

All data and documentation shall be made available to authorized persons promptly on request and without undue delays. Authorized persons are e.g. competent authorities or public prosecutors, the FIAU/FIU, etc.