GLOBAL ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM POLICY

sportradar

Table of Contents

1. Statement and Purpose

Sportradar AG and its subsidiaries (**"Sportradar"** or the **"Company"**) is committed to compliance with applicable laws and regulations, and to maintaining the highest ethical standards. In connection with the Company's Global Due Diligence Policy, Sportradar has adopted these Anti-Money Laundering and Counter-Terrorism Financing Policy (the **"AML Policy"**) to facilitate compliance with all applicable laws and regulations regarding the prevention of money laundering and any activities that facilitate the funding of terrorism or other criminal conduct.

The AML Policy and the internal controls herein set out:

- Sportradar's commitment to combatting the risk of its business being used to facilitate money laundering, terrorism financing or other criminal conduct;
- Sportradar employees' obligations to comply with the AML Policy; and
- How to recognize and report potential money laundering or terrorism financing.

Sportradar will not conduct business with individuals or entities whose conduct gives rise to suspicions of involvement with illegal activities. Sportradar will report suspected money laundering or terrorism financing activity to the relevant authorities. Questions you may have regarding the application of this Policy or AML to any contemplated transaction, dealing or activity should be promptly raised with a member of the Compliance Team.

Actual or suspected violations of this Policy should be reported to the Chief Regulatory and Compliance Officer or the Ethics Hotline. Reports may be made anonymously. Sportradar strictly prohibits retaliation, in any form, for the reporting of any actual or suspected violation.

2. Scope

The AML Policy is global in scope and applies to all employees, officers, and directors, consultants, contractors and service providers of Sportradar and its subsidiaries worldwide. The Policy applies in all countries where Sportradar conducts business, whether or not Sportradar has a physical presence in the country, i.e., an office. In the event of a conflict between applicable laws or policies and the AML Policy, we will apply the more stringent standard.

The AML Policy shall be utilized in conjunction with other internal policies.

3. Definitions

For purposes of the AML Policy, the following definitions apply:

- **Money Laundering:** engaging in acts designed to conceal or disguise the true origins of illegally or criminally-derived proceeds so that the proceeds appear to have legitimate origins or to be legitimate assets, and are thus introduced into the legal financial and business cycle.

    - **Terrorism Financing:** the provision of funds or providing financial support to individual terrorists or terrorist organizations.

- **Other Criminal Activity**: The provision of funds or financial support to further criminal activity of any kind.

- **Politically Exposed Person** (**"PEP"**) is an individual who is or has been entrusted domestically or by a foreign country with prominent public functions, for example head of State, head of government, minister and deputy or assistant minister; a member of parliament or of a similar legislative body; a member of a governing body of a political party; a member of a supreme court; a member of a court of auditors or of the board of a central bank; an ambassador, a chargé d'affaires and a high-ranking officer in the armed forces; a member of an administrative, management or supervisory body of a State-owned enterprise; a director, deputy director and member of the board or equivalent function of an international organization, except middle-ranking or more junior officials; this includes family members or close associates of such parties. Family member(s) is/are: the spouse, or a person considered to be equivalent to a spouse, of a PEP; the children and their spouses, or persons considered to be equivalent to a spouse, of a PEP, the parents of a PEP. Close associates are individuals who are closely connected to a PEP, either socially or professionally.

- **Ultimate Beneficial Owner** (**"UBO"**)**:** any natural person(s) owning or controlling through direct or indirect means at least 25% of the Company and/or natural person(s) who control(s) the Company by any other means (e.g., shareholders' agreement, the power to appoint members of the management board, veto right). If there is no identifiable natural person, the Director or senior level officer who would have control over significant business decisions and operations shall be identified for the purposes of the UBO identification.

4. Processes and Procedures

Sportradar shall maintain processes and procedures designed to ensure compliance with applicable AML and counter-terrorism financing laws and regulations, including, for example:

4.1 Customer Due Diligence (KYC)

Before entering into any business relationship with a current or prospective client, Sportradar requires completion of due diligence, including Know-Your-Customer ("KYC") procedures, which requires, among other things, the completion of a KYC Questionnaire. This questionnaire is designed to obtain information regarding the nature of the customer's business, corporate structure, significant shareholders, UBOs, directors, officers and other persons authorized to represent the customer, regulatory and licensing status, risk mitigating factors taken by the customer, and other details as deemed necessary by Sportradar's Compliance Team to complete an adequate review.

For additional information regarding procedures for conducting this due diligence, see Sportradar's Global Customer Due Diligence Policy.

4.2 Third-Party Due Diligence

Sportradar has also established procedures for conducting risk-based due diligence on all Third Parties, including Vendors and Representatives, to ensure that such Third Parties that Sportradar enters a business relationship with are appropriate and legitimate for their contemplated role, that they do not have any improper or suspicious connections or ownership interests, and are not likely to engage in any improper, unethical, corrupt, or illegal activities.

For additional information regarding procedures for conducting this due diligence, see Sportradar's Global Customer Due Diligence Policy and Vendors and Representatives Retention Policy.

4.3 Enhanced Due Diligence

Where necessary, Sportradar will conduct Enhanced Due Diligence ("EDD") on customers found to have a moderate risk or high-risk of potential involvement, either directly or indirectly, with money laundering, terrorism financing or illegal activity. EDD will be conducted in all situations where Sportradar may enter a business relationship with a PEP, where a PEP or a Sanctioned Person holds a position as an officer and/or as a shareholder or UBO of a potential customer, and/or where a PEP is directly or indirectly involved in a specific transaction.

EDD will follow the same components of a standard Customer Due Diligence but with stricter guidelines in certain components, specifically with regard to financial information requests. Under the KYC component, in addition to regular requests, Sportradar will request that the Customer provide additional information regarding the source of funds, e.g. bank statements or audited business accounts, particularly if the client is considered higher risk. Further, Sportradar will not only identify and verify the UBOs of the Customer, but also identify and verify the UBOs of representatives of the Customer (e.g. by requesting the extract form the UBO register), if applicable. EDD findings will be documented and analysed to determine appropriate measures for ongoing monitoring of the subject business relationship.

4.4 Sanctions Screening

Each party, entity or individual, identified during the KYC and third-party due diligence processes will be screened against Sanction Lists.

Sportradar will screen for compliance with appropriate agencies, including FinCEN and the Office of Foreign Assets Control ("OFAC") in the US, and the EU/UK asset-freeze sanctions regimes.

Sportradar has committed to not doing business with individuals or entities who are sanctioned by OFAC or appear on the Specially Designated Nationals (SDN) or EU/UK asset-freeze sanctions lists. Sportradar will comply with legal and regulatory requirements related to sanctioned entities.

Sportradar refuses to accept funds from, or disburse funds to, any entity or individual who appears on any OFAC SDN list as well as with any business that is 50% or more owned by an individual or entity who appears on the SDN list. Sportradar refuses to accept funds from, or disburse funds to, entities, shell companies, or customers whose funds are reasonably believed to have derived from or contributed to any criminal activity from a sanctioned source.

For additional information regarding procedures for conducting sanctions screening, see Sportradar's Global Trade Controls Policy.

4.5 Contract protections

Where possible, Sportradar shall introduce provisions in contracts with customers and third parties to include a commitment to comply with AML laws and regulations, and Sportradar's right to immediately terminate the contract in case of violation, subject to applicable law.

5. Red Flags

Sportradar employees should be vigilant in looking for warning signs, or red flags, that a customer, third party or transaction may need to be reviewed to ensure that it complies with applicable laws and this AML Policy. Employees must promptly report known or suspected violations of laws, rules, regulations or this Policy to the Chief Regulatory and Compliance Officer. Any such report shall be promptly reported to the Ethics Hotline. Employees may also report such violations directly through the Ethics Hotline website: EthicsPoint - Sportradar

Red flags include, but are not limited to, the following examples:

- Transactions which have no apparent business purpose and/or make no obvious economic sense;
- A party intends to make payments in cash or cash equivalents;
- A party engages in transactions that, without reasonable explanation, are out of the ordinary range of services normally requested;
- A party refuses to disclose or provide documentation concerning identity, nature of business, or nature and source of assets;
- A party has assets that are well beyond its known income or resources;
- A party is an entity without a clear registered office, does not appear online and refuses to disclose the identity of the party's beneficial owner;
- A party requests monetary transfers to or from a country other than the one in which the party is located and is unable to provide sufficient legitimate and independently verifiable justification for such request;
- A party requests monetary transfers to or from an unrelated third party and is unable to provide sufficient legitimate and independently verifiable justification for such request;
- A party requests that a transaction be processed in a manner that circumvents a Company procedure or avoids Company documentation requirements;
- A party is based in a high-risk country or country known as a tax haven;
- A party is a trust, shell company or private investment company that is reluctant to provide information on controlling parties and underlying beneficiaries;
- A party refuses to comply with the principles set forth in Sportradar's Code of Conduct, Anti-Bribery and Anti-Corruption Policy, or Sanctions, Export Control, and Antiboycott Policy.
- A party is owned or controlled by, or otherwise closely affiliated with, a PEP or a Sanctioned Person.

6. Risk Assessment

Sportradar employs a risk-based approach to combatting money laundering and terrorism financing. The risk assessment is a critical component of Sportradar's AML compliance program. As part of its risk-based approach, the Compliance Team shall conduct an AML risk assessment to identify and understand the risks specific to Sportradar and its business. The risk profile will be determined by identifying and documenting the risks inherent to the Company including Sportradar's products and services offered, customers, transactions, payment channels, the geographic locations in which it operates, and other qualitative and emerging risks, in accordance with standard risk assessment methodology. The Compliance Team will also assess the effectiveness of Sportradar's internal controls to manage and mitigate the risks of money laundering and terrorism financing. The selection of risk categories and the weight given to each in an AML risk assessment will vary depending on the circumstances.

The Compliance Team shall update the risk assessment on a periodic basis, at least annually, to reflect variations in any risk profiles that occur due to changes in Sportradar's business, regulatory requirements, industry guidance, or other emerging risks that would materially impact the risk assessment.

7. Suspicious Activity Reporting Requirements

In accordance with applicable laws and regulations, Sportradar will, where required, report any suspicions of money laundering or terrorism financing activity to the Financial Intelligence Units or other relevant authorities in jurisdictions where Sportradar holds a gaming or sports betting-related license, certification or approval. See Appendix A for additional information.

8. Reporting Concerns

The prevention and reporting of any form of money laundering or terrorism financing is the responsibility of all employees.

Employees should notify the Chief Regulatory and Compliance Officer immediately if they become aware of a suspected violation of the law or the AML Policy, including if they reasonably suspect that one of their colleagues or other individuals closely affiliated with Sportradar are engaging in actions that constitute money laundering or facilitate the commission of money laundering. The reporting of potential breaches can be reported verbally, in writing or per telephone.

Employees may also report such violations directly through the Ethics Hotline website. They should refer to and follow Sportradar's Ethics Hotline reporting procedure in making their report.

EthicsPoint - Sportradar

Consistent with applicable laws and regulations, the Company will take appropriate steps to investigate all concerns reported in good faith, and to protect the anonymity of any employee that submits a complaint anonymously and indicates a desire to remain anonymous.

The Company is committed to ensuring that employees who refuse to take part in money laundering, who report in good faith their concerns regarding any actual or potential violation of this Policy or applicable AML Laws, or who assist in the Company in investigating the same, are protected from retaliation.

Any employee found to have engaged in any such retaliation shall have violated this Policy and will be subject to appropriate disciplinary action.

9. Record-Keeping and Document Retention

The Chief Regulatory and Compliance Officer is responsible for keeping records related to AML compliance. Copies of documents and information deemed necessary to comply with regulatory AML standards will be kept for a general period of 5 years, or longer, as required by law after the end of the business relationship or as governed by a regulatory body. Furthermore, Sportradar reserves the right to extend general retention period by an additional 6 months to allow for due notification by courts in case of a claim against the Group.

Sportradar and all of its personnel are required to make and keep books and records that accurately and fairly reflect the transactions of the Company, and to devise and maintain an adequate system of internal accounting controls in accordance with all applicable laws and relevant Sportradar policies and procedures.

All third party payment arrangements must, among other things, reflect the true nature of the transaction. The underlying supporting documentation for any payments made to third parties must adequately support and reflect the true nature of the transaction, as well. Sportradar personnel are prohibited from creating or maintaining inaccurate Company records relating to the Company's payments to and from third parties.

10. Awareness and Training

Sportradar requires that relevant employees participate in training on this Policy. Existing employees will receive periodic training on this Policy, in line with any updates to governing legislation and legal requirements, as appropriate.

11. Monitoring and Review

The Compliance team will monitor and review compliance with the Policy through regular Compliance reviews and periodic assessments. The Compliance Team is hereby authorized to amend and update this Policy as needed to remain in compliance with all applicable rules, laws, regulations, and international treaties. Employees and third parties are responsible for understanding or seeking clarification of any rules outlined in this document and for familiarizing themselves with the most current version of the Policy.

12. Deviations

No exemptions from this Policy can be granted unless there are exceptional circumstances. All requests for exemptions must be made in writing to the Compliance Team. The Compliance Team must assess and decide on each request individually. Exemptions must be duly logged and documented.

These policies are not designed to answer every question that may arise, but instead serve as a set of guiding principles for a constantly changing business environment. Questions regarding these policies can be directed to any member of the Company's Compliance Team.

Document Information:

Document	
Version	**V.1**
Contact person	**Anja Martin, Chief Regulatory and Compliance Officer**
Approved by	**Carsten Koerl, CEO** **Alexander Gersh, CFO** **Lynn McCreary, CLO**
Effective date	**28.07.2021**
Area of application	**All Sportradar Group Companies**

Appendix A

Suspicious Activity and Large Currency Transaction Reporting

Jurisdiction	Monetary Amount for Required Report	Government Agencies for Reporting	Additional Reporting Requirements
United States	$10,000	Internal Revenue Service; and Financial Crimes Enforcement Network (FinCEN)	Report of cash payments over $10,000 received in a trade or business must be filed by submitting IRS Form 8300. Sportradar is not required to file suspicious activity reports under the Bank Secrecy Act of the United States.
United Kingdom	£10,000	U.K. Financial Intelligence Unit; and National Crime Agency	All SARs are filed through the NCA's online portal.
Belgium	Sportradar does not have suspicious activity or large currency transaction reporting obligations in this country.		
Greece	€15,000	Hellenic Financial Intelligence Unit	Suspicious transactions must be reported immediately along with supporting documentation.

Malta	Sportradar does not have suspicious activity or large currency transaction reporting obligations in this country.		
Romania	Sportradar does not have suspicious activity or large currency transaction reporting obligations in this country.		
Denmark	Any amount (if you reasonably suspect money laundering).	State Prosecutor for Serious Economic Crime	
Slovakia	Sportradar does not have suspicious activity or large currency transaction reporting obligations in this country.		
Gibraltar	Any amount (if you reasonably suspect money laundering).	Gibraltar Financial Intelligence Unit	Must also report suspicions/knowledge of money laundering or other illegal activity with the Gambling Commissioner within 24 hours.