Flutter™

Sanctions Policy

Applicability: Global

Issuing function: Legal & Commercial

A message from Flutter Chief Legal Officer

"Building a culture where we operate responsibly, honestly, fairly and in accordance with the laws in each of the jurisdictions in which we operate is essential to us at Flutter. It is the responsibility of everyone at every level to help build and maintain this culture by being aware of and understanding the Sanctions risks that face our business. This responsibility includes adhering to the requirements set out in this Policy. Thank you for taking the time to read and understand this Policy and for helping Flutter build and maintain a culture we can all be proud of."

I. Introduction, Purpose and Scope

Flutter Entertainment plc, and all of its subsidiaries ("Flutter"), is committed to conducting business honestly, fairly, and with respect for people in accordance with the law in each of the jurisdictions in which it operates. The purpose of this Policy is to outline:

I. What Sanctions are;
II. Our approach to managing sanctions risks throughout our business;
III. What your responsibilities are to guiding against Sanctions risks; and
IV. The steps we all must follow when a possible or actual Policy violation occurs.

This Policy applies to Flutter employees as well as board members, agency workers, volunteers, independent contractors and third parties working on behalf of the company (hereinafter to be referred to as "you").

This Policy is supported by the supplementary documentation outlined in section VI.

This Policy has been approved by the Risk and Sustainability Committee (RSC) or its designate. It will be reviewed and updated on an annual basis and, if necessary, more frequently where regulations/business changes require it.

II. Statement of Policy

Key definitions

Sanctions: Consist of a wide range of political and/or economic measures which are imposed by governments with the intention of influencing the behaviour of a particular country's regime, individuals, or groups. The types of sanctions measures put in place can vary widely, including, financial restrictions, import/export restrictions and travel bans. The following are some examples of countries/territories and groups that are the subject of comprehensive and targeted Sanctions:

- Russia
- North Korea
- Cuba
- Iran
- Syria
- Crimea
- Donetsk
- Luhansk
- Narcotics traffickers
- Terrorist organisations
- Human rights abusers

Our approach to Sanctions

Flutter is committed to complying with all economic and trade Sanction laws and regulations in the jurisdictions in which we operates, by preventing the use of our products or systems that evade sanctions, or to bypass applicable sanction laws. We reserve the right to suspend any customer or third-party relationship that is deemed contrary to relevant laws. To help ensure that we do business in a compliant manner, we have implemented the following:

- Policies, standards, and training to ensure understanding of what sanctions are and what their roles and responsibilities are in mitigating our business risks;
- Formal escalation channels to flag suspicions of possible or actual Sanctions Policy violations; and
- Frameworks and procedures designed to continuously monitor for and prevent Sanctions risks in our global operations.

Summary of Flutter's Sanction's standards

This Policy is supported by standards. The standards seek to establish a benchmark that is met consistently across all subsidiaries. Flutter's Sanctions standards define (non-exhaustively):

Tone from the top	IT system requirements
Governance and oversight	Third party due diligence
Training and awareness	Exiting relationships
Business risk assessments	Internal and external reporting
Customer due diligence	Record-keeping
Employee due diligence	Independent program reviews

Common red flags that you should look out for

Sometimes, individuals and companies who are sanctioned will try and conceal their true identify in order to get around the controls we have in place to detect and prohibit engagement with them. You must look out for, and report red flags you come across in line with your local Sanctions procedures and escalation channels including:

- At onboarding account opening, information that is misleading, vague, difficult to verify in an attempt to conceal their true identity or evade our onboarding procedures;
- A counterparty has a different name or location than a customer or ultimate end user;
- Unusual invoicing, packaging, and shipping requests that do not align with Flutter's standard business procedures;
- Documents, including contracts, requests to bid, letters of credit, purchase orders, shipping and customs documents, certificates of origin and questionnaires that include words such as "boycott", "blacklist", "whitelist" or similar terms;
- Suspicion or evidence indicating the possible involvement of a Sanctioned territory or party; or
- Surprisingly favourable payment terms or large cash payments.

Issued by: Group Financial Crime
Highest approval authority: RSC
Approval date: 10 Dec 2024

Version: 4.0
Information classification scale: Public
Document ID: Flutter Sanctions Policy - ENG

III. Roles and Responsibilities

Employees must:

- Familiarise yourself with the content of this Policy;
- Ensure you complete the relevant training within the time frames allocated;
- Follow guidance from our Procurement, Human Resource and Financial Crime teams when engaging a customer, employee or third party to ensure appropriate background checks are completed;
- Understand your obligations to identify and escalate red flags or escalate where you are unclear;
- Report any breach or wrongdoing (past, present, or likely future);
- When in doubt, seek guidance from your line manager and local Financial Crime team.

Company management must:

- Communicate this Policy to your team to ensure awareness;
- Ensure your team understand their obligations to identify and escalate red flags where appropriate;
- Ensure your team have access to and are assigned all relevant trainings;
- Monitor compliance within your team to ensure training is completed in the allocated time frame;
- Report any breach or wrongdoing (past, present, or likely future).

You should be aware that failure to comply with this Policy could result in disciplinary action up to, and including, termination of employment or a business relationship, if deemed appropriate by Compliance, HR or relevant line management.

IV. Monitoring, Assurance and Breach Reporting

Compliance with this Policy is monitored, and assurance activities are performed at regular intervals. You should raise any concern with someone who can help address them properly, namely your Financial Crime team. Depending on the circumstances, you may choose to report internally or externally via our Independent Confidential Reporting Service.

You should raise any concern with someone who can help address them properly. Your Compliance team may be in the best position to address concerns over potential breaches of this policy. You can also reach out on this matter to your line manager or other trusted persons such as Flutter's own Legal Counsel or Internal Audit. Where it is not possible or desirable to address a particular concern in consultation with your line manager, or where a reportable matter continues to be unresolved following consultation, you should submit a report about a reportable matter through the Speak-Up platform. Please refer to our Whistleblowing policy for details.

V. Relevant Contact Details

In the event of any questions with regards to the content, context or meaning of this document please contact:

Responsibility	**Name**	**Email**
Group Financial Crime	The Financial Crime Team	GroupFinancialCrime@flutter.com

VI. Supplementary Documentation

- Flutter Code of Ethics
- Flutter Whistleblowing Policy
- Flutter AML & CFT Policy
- Flutter Anti-Bribery and Corruption Policy
- Conflict of Interest Policy
- Flutter Gifts and Hospitality Policy

For Flutter employees, please refer to your local intranet for more information and access to supportive material.