Sisal Whistleblowing Policy

Approved by the Sisal Board of Directors on 24/06/2024

Table of contents

FOREWORD

Sisal S.p.A. (“Sisal” or the “Company”) and its subsidiaries are committed to conducting their business activities with honesty and integrity, maintaining the highest standards of conduct and ethical behaviour, also in line with the principles dictated by the parent company Flutter Entertainment PLC (“Flutter”) and applicable to all its subsidiaries (the “Group”).

With the aim of promoting and reinforcing these standards, Sisal has implemented a Whistleblowing Policy (hereinafter also the “Policy”) for the reporting of any conduct, including omissions, which constitutes or may constitute a violation or inducement to a violation of laws, regulations, values and principles sanctioned by its Code of Ethics and Conduct, Model 231, its own corporate policies and procedures or the Group’s policies and procedures, as better specified in the paragraph “PURPOSE AND SCOPE”. Anyone is invited to give prompt notice of such conduct by means of the methods described below, refraining from undertaking autonomous initiatives of analysis and/or investigation.

For this reason, the Company has implemented specific communication channels for the handling of Whistleblowing reports (as defined below) in order to be compliant with Legislative Decree No. 24/2023 which implements the Directive (EU) 2019/1937 as well as with the whistleblowing principles laid down in Flutter’s “Whistleblower Policy”.

To this end, this Policy:

- defines the scope of the Whistleblowing process;
- identifies the persons who may make Reports;
- identifies the channels through which the Report may be made, appropriate to guarantee the confidentiality of its content;
- identifies and lays down the principles and general rules governing the Whistleblowing

process, as well as the consequences of any abuses in the use of the established channels;

- defines the Whistleblowing management process in its various phases, identifying roles, responsibilities, operating methods and tools used;
- defines the modalities for processing the content of the Report, including the identification data of the Whistleblower and the Reported Person;
- protects the Whistleblower against retaliatory and/or discriminatory conduct, direct or indirect, for reasons related to the Report.

PURPOSE AND SCOPE

This Policy describes the process and communication channels to be used for sending, receiving, analysing and processing Reports of irregularities or unlawful conduct, including omissions, committed or attempted, which constitute or may constitute:

a) a violation, or inducement to a violation, of laws and regulations relating in particular to the following areas:
   - public procurement;
   - financial services, products and markets and the prevention of money laundering and terrorist financing;
   - safety and conformity of products;
   - consumer protection;
   - protection of privacy and protection of personal data and security of networks and information systems;
   - public health;
   - environmental protection;
   - violations of competition and state aid rules;
   - violations of corporate tax rules;

b) a violation, or inducement to a violation, of internal legislation, such as:
   - values and principles laid down in Sisal's Code of Ethics and Code of Conduct, Flutter's Code of Ethics and any other Code of Ethics adopted by the International Division – which means the territorial division of the *UK & Ireland, International, US and Australia* Group to which the Company belongs;
   - values, principles and controls identified in Sisal's Organisation, Management and Control Model pursuant to Legislative Decree 231/2001;

- internal policies and procedures of Sisal and the Group, including Flutter's Anti-Corruption Policy; or

c) in general, a violation of national or European legislation, including that relating to gaming licences or the prevention of money laundering and terrorist financing.

Please refer to Appendix A at the end of this Policy for a more detailed illustration of the conduct that may the subject matter of reporting.

Reports that do not fall within the objective scope as identified above are addressed to the relevant departments (e.g. reports of malfunctions, requests for product information, customer complaints, etc.).

DEFINITIONS AND ABBREVIATIONS

CHANNELS FOR REPORTING: Communication channels identified by Sisal as the means, internal or external to the organisation itself, for conveying reports.

WHISTLEBLOWING COMMITTEE or COMMITTEE: a committee composed of the Internal Audit Director and the Chief Risk & Compliance Officer, who have also been identified as Sisal's Confidential Designee, to express the appropriate evaluations in the event of Reports with a Determinant Impact having relevance at the parent company or divisional level (*i.e.* the *Material Impact and Serious Misconduct and Improper Behaviour* referred to in the "Whistleblower Policy" of Flutter).

ILLEGAL BEHAVIOUR: Any act or omission constituting or likely to constitute a violation or inducement to a violation in respect of the conduct set out in paragraph "PURPOSE AND SCOPE OF APPLICATION".

CONFIDENTIAL DESIGNEE: in accordance with Flutter's "Whistleblower Policy", these are the persons assigned responsibility for managing the whistleblowing investigation process.

SUPERVISORY BODY (Organismo di Vigilanza, hereinafter "OdV"): Supervisory Body pursuant to Legislative Decree 231/2001, is involved in evaluating reports relevant to Legislative Decree 231/01.

RETALIATION: any conduct, act or omission, even if only attempted or threatened, committed by reason of the Report and causing or likely to cause the Whistleblower, directly or indirectly, unjust damage.

WHISTLEBLOWER: Subject, among those referred to under "RECIPIENTS OF THE POLICY", who makes the Report.

REPORT: Communication by the Whistleblower concerning information on Illegal Behaviour.

REPORTED PERSON: Subject to whom the Whistleblower attributes the illegal conduct that is the subject matter of the Report.

REPORTS WITH SIGNIFICANT IMPACT: any violation of regulations or internal policies that has occurred or is likely to occur (with a probability of ≥50%) within the next three years and that could pose a serious, severe or critical risk to the Flutter Group.

SERIOUS MISCONDUCT AND IMPROPER BEHAVIOUR: (i) Reports with a Significant Impact, (ii) Reports concerning corrupt conduct, (iii) Reports that may have reputational consequences for the Group involving the media, investors or authorities, (iv) Reports concerning working conditions or misconduct in the workplace (e.g. threats of physical

violence, sexual, verbal or other harassment, discrimination, hostile environment, conflict of interest or substance abuse. This type of report requires a more in-depth investigation.

RECIPIENTS OF THE POLICY

This Policy applies to the following persons (hereinafter also referred to as "Recipients" and/or "Whistleblowers"):

a) Group workers (employees, self-employed, volunteers, paid and unpaid trainees, former employees[1], job applicants[2]);
b) shareholders and members of the administrative, management or supervisory body of a company, including non-executive members, volunteers and paid and unpaid trainees;
c) any person working under the supervision and direction of contractors, subcontractors and suppliers, customers, partners, consultants and, more generally, the Group's stakeholders.

[1] If they report or disclose information on violations acquired in the context of the terminated employment relationship.

[2] If their employment relationship has not yet commenced and information concerning the violation has been acquired during the selection process or in pre-contract negotiations.

GENERAL PRINCIPLES

The Whistleblowing system is inspired by the following fundamental principles:

- **Protecting the identity of Whistleblowers and the confidentiality of information**: the identity of the Whistleblower is always protected and kept confidential by processing the data in accordance with the law and taking all useful measures to prevent the dissemination of the Whistleblower's data and the content of the Report. Sisal guarantees that the identity of the Whistleblower will not be disclosed - without his/her explicit consent - to anyone who is not part of the authorised personnel competent to receive and follow up Reports, unless disclosure is a necessary and proportionate obligation imposed by EU or national law.

  In particular, the duty of confidentiality is waived in cases where:

  (i) in disciplinary proceedings, the dispute is based, in whole or in part, on the Report and knowledge of the identity of the Whistleblower is indispensable for the accused's defence; and

  (ii) the disclosure of the identity of the Whistleblower and of information from which that identity may be inferred, directly or indirectly, is also indispensable for the defence of the person concerned.

  In such cases, the Whistleblower shall be notified, in writing, of the reasons for the disclosure of the confidential data. Furthermore, the Reports are exempt from the right of access provided for, and to the extent applicable to the private sector, by Articles 22 et seq. of Law no. 241/1990, as well as by Articles 5 et seq. of Legislative Decree no. 33/2013. The measures to protect the confidentiality of the Whistleblower are aimed, inter alia, at ensuring that he/she is not subject to any form of retaliation.

Outside the cases identified above, anyone who fails to comply with the obligation of confidentiality will be subject to disciplinary measures, up to and including dismissal, in accordance with the current disciplinary system.

- **Prohibition of retaliatory or discriminatory acts against Whistleblowers**: the Company prohibits any form of retaliation or discrimination, whether active or omissive, even if only attempted or threatened, carried out as a result of the Whistleblowing and which causes or may cause the Whistleblower, directly or indirectly, unjust damage. This protection is guaranteed if the Report (even if subsequently assessed as unfounded) was made in good faith, because the Whistleblower had reasonable grounds to believe that the information on the reported violations was true at the time of the Report and that it fell within the objective scope of this Policy.

  Discriminatory measures include unjustified disciplinary actions, harassment in the workplace and any other form of retaliation that results in intolerable working conditions for the Whistleblower; an example of possible discriminatory measures is contained in Appendix B to this Policy.

  Sisal guarantees the removal of the effects of any form of retaliation against the Whistleblower.

  The commission of retaliatory or discriminatory acts against any person who has made a Report in accordance with the provisions of this Policy shall entail the initiation of disciplinary proceedings against the perpetrator of such acts and the imposition of the relevant disciplinary measures (which may also entail dismissal), in accordance with the provisions of the applicable national labour law, and shall be reported to the

competent authorities, in accordance with the provisions of the applicable legislation, and the persons responsible may be subject to civil and criminal penalties.

It should also be noted that the measures listed above for the protection of Whistleblowers also apply, where appropriate, to the persons and situations referred to in Appendix C.

Therefore, anyone who believes that he or she has suffered retaliation/discrimination on the above-mentioned grounds must file a report on the retaliation/discrimination suffered. In such cases, the Company ensures that the relevant investigations are carried out promptly.

The Whistleblower cannot be held liable for defamation, violation of copyright, secrecy obligations, data protection rules and disclosure of trade secrets. No liability can be attributed to the Whistleblower even in relation to the conduct adopted to access the information that is the subject of the Report. In addition, the persons concerned have the right to legal protection in the event of criminal or civil liability on the part of the Whistleblower in connection with the falsehood of what has been declared or reported.

Should, on the contrary, the reports prove to be manifestly unfounded, made with malicious intent or gross negligence, or should the Whistleblower be found liable for the offences of defamation or slander, such a condition would constitute a breach of this *Policy*, with the possible application of disciplinary measures and recognition of liability on the part of the Whistleblower; in such cases, the protections against the Whistleblower set out in this paragraph could not be guaranteed.

- **Protection of the Reported Person**: the Company protects Reported Persons as regards both the confidentiality of the reports concerning them and of any

investigations carried out, and the protection of the same from any retaliatory and/or defamatory actions.

After investigating the merits of the Report, the Committee, if disciplinary proceedings are opened, informs the person to whom the Report refers and keeps him/her up-to-date on the progress of the proceedings, compatibly with the performance of the necessary verification and evidence-gathering activities, so as to enable him/her to exercise his/her right of defence.

The Reported Person's personal data may be transmitted to the competent administrative or judicial authorities and, more generally, to public bodies, in compliance with the formalities laid down by law, or in order to comply with requests received from them.

- **Protecting the integrity of Reports**: the *web* platform ensures that no Reports (from notification to decision) can be deleted and/or altered.

- **Duty of independence and professionalism in the management and assessment of Reports**: all persons involved, in any capacity whatsoever, in the process of managing and assessing Reports must perform their duties in compliance with the duties of independence and ensuring the accurate and efficient management and assessment of all Reports. In particular, the body in charge of handling Reports is autonomous, dedicated and composed of staff specifically trained for this activity.

THE WHISTLEBLOWING SYSTEM

The Companies' whistleblowing system consists of the following channels:

a) web platform accessible 24/7 at the following link [LINK] that guarantees the non-tracking and registration of the IP addresses of the Whistleblowers;

b) registered telephone line/voice messaging system accessible 24/7 at the following telephone number 800761667; and

c) direct meeting through a request to the Whistleblowing Committee.

The Company recommends that Reports be sent via the *web* platform, as it is specifically designed to guarantee ease of use, privacy and confidentiality for the Whistleblower and - in the case of an anonymous Report - to allow clarifications to be sought from the Whistleblower, while maintaining his/her anonymity.

If the recorded telephone line/voice messaging system is used for the Report or a face-to-face meeting is requested, the Whistleblowing Committee may request, with the consent of the Whistleblower, that the Report be documented (as the case may be by means of a verbatim transcript, recording of the conversation, detailed report or minutes).

The Whistleblower is given the opportunity to verify, rectify and approve, as appropriate, the transcript, report or minutes of the meeting.

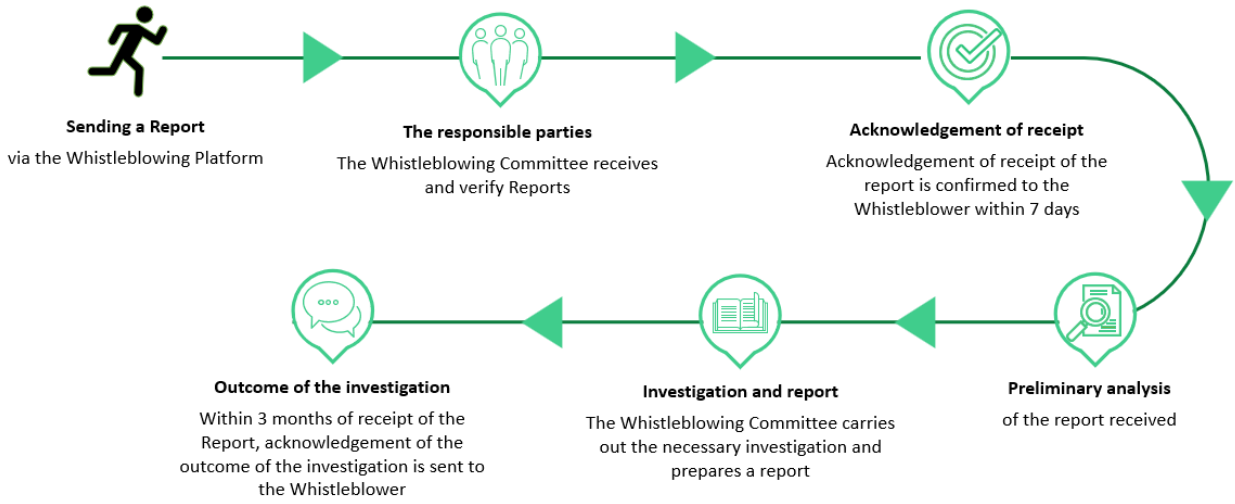
It should be noted that transcripts, reports or minutes of Reports received through internal channels other than the *web* platform are also entered into the platform by the Whistleblowing Committee.

For the subsequent steps in the handling of such Reports, the following paragraphs apply.

In any case, anyone who receives a Report through channels other than those provided for by the Reporting system must promptly - and no later than 7 (seven) days after the Report - forward it in original with any attachments to the Whistleblowing Committee, which will enter it in the *web* platform, with simultaneous notice of the transmission to the Whistleblower.

The transmission must be carried out with the utmost confidentiality and in such a way as to protect the Whistleblower and the identity of the Reported Persons, without prejudice to the effectiveness of the subsequent investigation activities. No copies of the Report should be made.

THE REPORTING PROCESS



Reporting unlawful conduct

Sisal encourages the persons referred to in the “RECIPIENTS OF THE POLICY“ to report irregularities or unlawful conduct, including potential ones, of which they become aware, using the channels provided by the Reporting System, so that they can be verified by the competent bodies.

Awareness or mere suspicion of the commission of unlawful conduct may manifest itself in the performance of the duties of Group employees in dealings with internal or external personnel, law enforcement agencies, regulatory agencies, customers or other third parties. Reports may be made anonymously, but Sisal recommends that they be made by name, in order to allow the persons in charge to carry out a more efficient investigation, applying in any case the protections provided against possible retaliation. In any case, if the Report is

anonymous, all the persons involved in receiving and/or assessing it shall take all the necessary precautions to ensure the anonymity of the Whistleblower, refraining from any attempt to identify the Whistleblower or reveal his/her identity, unless required by law.

The Report must be made in good faith. The Whistleblower is invited to provide all the elements in his or her knowledge, useful to proceed with the necessary and appropriate verifications to confirm the validity of the facts subject of the Report, attaching the documentation supporting the potential unlawful conduct subject of the Report in the possession of the Whistleblower.

It is particularly important that it includes, where these elements are known to the Whistleblower:

- a detailed description of the facts that occurred and how they became known;
- date and place where the event occurred;
- name and role of the persons involved or elements that might enable them to be identified;
- names of any other persons who may report on the facts that are the subject of the Report or elements that may enable them to be identified;
- reference to any documents that may confirm the accuracy of the reported facts.

The Whistleblower should take care not to report information that is irrelevant or unnecessary to the Report.

Reports that do not meet the requirements identified above are dismissed for lack of essential elements.

All Reports are received and managed by the Whistleblowing Committee, appointed as authorised persons to process and duly instructed in the processing of personal data

pursuant to Articles 29 and 32(4) of Regulation (EU) 2016/679 and Article 2-quaterdecies of Legislative Decree 196 of 2003.

The Whistleblowing Committee informs the OdV of Reports concerning the Model pursuant to Legislative Decree no. 231/2001, in order to ensure the involvement of the OdV in assessing and deciding on such Reports. The Whistleblowing Committee is responsible for interacting with the Whistleblower in compliance with the deadlines laid down by law.

Reports intended to expose situations of an exclusively personal nature and outside the scope of the legal provisions are not taken into account.

Moreover, if the Whistleblower makes a report, he/she may be held liable in cases where the Report proves to be, due to wilful misconduct or gross negligence, false, unfounded and/or made for the sole purpose of harming the Reported Person. In more serious cases (e.g. wilful misconduct in the falsehood of the report), the conduct may be subject to disciplinary proceedings under Law No. 300/70 or cause termination of the contract or appointment.

Whistleblowing Platform

The Whistleblowing Platform ensures traceability of the Reporting workflow.

All information in the Report is protected to ensure maximum confidentiality and accessible only by the Committee or persons expressly authorised by it.

The Platform is made available to the Recipients through the Speak Up! website or via the corporate intranet. When a Report is sent, after having read the information on the processing of personal data, the Whistleblowing Platform issues a token (Report ID), which can be used by the Whistleblower to obtain information on the outcome of the Report and to ensure communications also in total anonymity.

In addition, the Whistleblowing Platform provides for the possibility for the Whistleblower to exclude internal Functions from the management and assessment of the Report, if they are directly involved in the Report. For further details on the management of conflicts of interest, please refer to the dedicated section of this Policy.

The Whistleblowing Committee accesses the Platform to consult all Reports received and to carry out the relevant activities. All the accesses are tracked and the Platform is protected by appropriate technical security measures.

Reports received outside the prescribed channels

The Sisal Function receiving a Report made outside the prescribed channels must forward it without delay, in original with any attachments, to the Whistleblowing Committee, which will take care of entering it into the Platform. The transmission must be carried out with the utmost confidentiality and in such a way as to protect the Whistleblower and the identity of

the Reported Persons, without prejudice to the effectiveness of the subsequent investigation activities. No copying, forwarding or printing of the Report received should be carried out.

Preliminary analysis

The Reports are subject to preliminary analysis by the Whistleblowing Committee, with the possible involvement of the OdV in the case of relevant Reports pursuant to Legislative Decree 231/2001. The Whistleblowing Committee verifies the presence of useful data and information to allow an initial assessment of the Report. Within 7 (seven) days of receipt of the Report, the Committee sends the Whistleblower an acknowledgement of receipt of the Report, using the communication methods adopted by the Whistleblower for sending the Report.

The Committee, as part of its preliminary analysis and execution of the investigation, takes into consideration whether there are any common themes or repeated allegations concerning a particular department or individual involved in an investigation.

The Committee takes all necessary measures to treat Reports in a confidential manner, also with a view to protecting the identity of the Whistleblower, the Reported Person and other persons mentioned in the Report.

In the course of its verifications, the Committee may avail itself of the support of the competent corporate functions from time to time (e.g. the HR Function) and, where deemed appropriate, of external consultants specialised in the field of the Report received and whose involvement is functional to the investigation of the Report, ensuring the confidentiality and anonymisation of any personal data contained in the Report.

Anyone involved in the verification activities related to a Report is required to cooperate fully and to follow the instructions received in carrying out their activities.

All persons involved in the inspections must maintain strict confidentiality regarding information received during the inspections.

At the end of the preliminary analysis, the Committee may:

a) dismiss the Report as insufficiently supported by evidence, manifestly unfounded or relating to conduct or facts not relevant to this Policy;
b) open the investigation phase as described in the following paragraph, involving the OdV in the case of relevant Reports pursuant to Legislative Decree 231/2001; or
c) involve Flutter's Confidential Designee (or a different person if the same is in a situation of conflict of interest) for the appropriate assessments in case of Reports with a Determinant Impact and/or Serious Violations and Misconduct or otherwise deemed by the Committee to be relevant at Group level.
   In the event of escalation to Flutter's Confidential Designee, the rules of Flutter's relevant regulatory instruments will apply.

In making its assessment of the need to open the investigation phase, the Committee must consider, among others, the following elements:

- the identity of the Reported Person: e.g. Reports made against a *senior member* of Group staff may require a more extensive investigation;
- the nature of the violation being reported: it may be appropriate to include a senior member of the HR Department, Finance, depending on the area of expertise, in the team that will take part in the investigation; if necessary, external consultants, forensic experts or other types of professionals may be involved in the Committee's

investigation;

- the circumstance that the reported facts concern a violation of accounting or internal controls and internal auditing (in particular if relevant under the Sarbanes-Oxley Act or rules imposed by the SEC): these types of Reports may require the involvement of Flutter's Audit Committee where necessary;
- the seriousness of the Report: the more serious the Report appears, the more accurate its assessment must be. For example, Reports relating to corruption, financial statements integrity or which threaten the Group's reputation, involve investors or which relate to employment conditions (physical, verbal, sexual violence or harassment, discrimination, hostile treatment, conflicts of interest or abuse of drugs in the workplace) are likely to require a more accurate assessment.

The Committee shall inform the Whistleblower of the outcome of the investigations carried out within a reasonable time limit, in any case not exceeding three (3) months.

If the Report indicates the occurrence of a violation of laws or regulations, with the prior authorisation/consultation of the Head of the Legal Function or of an external legal advisor and, where appropriate for reports relevant at Group level, in consultation with Flutter's Board Audit or Risk and Sustainability Committee, the Committee may report such circumstance to the competent authority.

Investigation

With reference to each Report, where, following the preliminary analysis, useful and sufficient elements emerge or are otherwise inferable to make an assessment of the merits of the Report, the Committee shall:

- initiate specific analyses, involving, where appropriate, the corporate functions concerned by the Report;
- terminate the investigation at any time if, in the course thereof, it is established that the Report is unfounded;
- check the possible legal implications for the Company;
- assess whether there is an obligation to inform the authorities;
- in the event that the conduct complained of continues, request precautionary measures to be taken to bring the conduct to an end.

At this stage, the Committee ranks the report according to the options on the Speak Up platform, which will then be reviewed after the investigation is closed.

In addition, the Committee must:

- ensure that the investigation is accurate, fair, impartial and protects the confidentiality of the identity of the Whistleblower and of the persons involved, including the Reported Person;
- ensure that appropriate measures are taken for the collection, processing and storage of personal information and ensure that the needs of the investigation are balanced with the need to protect privacy. On this point, it is the duty of the Whistleblowing

Committee to assess whether to inform the Reported Person about the investigation. The Reported Person is, however, always informed by the Whistleblowing Committee in the event of disciplinary proceedings;

- ensure that the investigation is carried out with the utmost speed and diligence.

Outcome of the investigation

At the end of the verification phase, the Committee prepares a report summarising the investigation carried out and the evidence that emerged, sharing it, on the basis of the results, with the persons from time to time competent, including the OdV in the case of Reports of relevance pursuant to Legislative Decree no. 231/2001, in order to define any intervention plans to be implemented and the actions to be taken to protect the Company and the Group, also communicating the results of the investigations and verifications carried out in relation to each Report to the heads of the corporate structures concerned by its contents.

The Committee classifies, within the Whistleblowing Platform, the analysed Report into:

1. Report lacking sufficient and relevant information;
2. Report unsubstantiated;
3. Report substantiated.

Should the conclusion of the analysis reveal the absence of sufficiently circumstantiated elements or, in any case, the unfounded nature of the facts referred to in the Report, the latter is filed by the Committee, together with the relevant reasons.

In the event of a well-founded Report, any remedial action shall be proportionate to the violation committed and take into account: (i) the seriousness of the violation; (ii) the possible

repeated commission of the violation; (iii) the intent of the infringer; (iv) the impact of the violation on Group personnel, the function concerned and the Group in general; and (v) any aggravating or mitigating circumstances. Any disciplinary action shall be taken in accordance with the local law applicable to the offender.

It is understood that, in all cases, upon completion of the verification of the merits of the Report received, the Whistleblower shall be provided with feedback within a reasonable time limit, in any case not exceeding three (3) months.

CONFLICT OF INTEREST

The handling and assessment of the Report must be entrusted exclusively to persons who are not in a situation of conflict of interest. Therefore:

a) if the conflict of interest situation relates to one or more members of the Committee, those members do not take part in the management of the case and the remaining members of the Committee must identify other suitable persons to restore the Committee's integrity;

b) if the conflict of interest situation concerns all the members of the Committee, the Report will be attributed to Flutter's Confidential Designee. If this is not possible, the Report will be forwarded to the Group Director of Compliance or the Group Chief People Officer. In any case, the members of the OdV must be kept informed of the progress of the handling of the report;

c) if the Report refers to one or more members of the OdV, the persons in conflict situations shall not take part in the assessments relating to the Report, and the OdV itself shall inform the Board of Directors, which shall assess the operating procedures to be followed and the corporate functions to be involved in the management of the Report.

These provisions also apply in the event that the conflict arises during the course of the inspection.

REPORTS

On a quarterly basis, the Committee provides the CEO, Flutter's Confidential Designee and the OdV with a summary report of all reports handled (filed and investigated), containing the results of the analysis, including the adoption (or non-adoption) of disciplinary measures.

In addition, the Internal Audit Function provides the OdV with a detailed monthly report on the progress of the investigations and assessments concerning the significant Reports pursuant to Legislative Decree 231/2001.

PROCESSING OF PERSONAL DATA

It should be noted that the personal data of the Whistleblower, the Reported Person and all the persons involved in the Report are processed in accordance with the current legislation on the protection of personal data set out in Regulation (EU) 2016/679 ("GDPR") and Legislative Decree 196/2003, as amended by Legislative Decree 101/2018. In particular, it is highlighted in this context that:

- the processing activities underlying the management of the Report are carried out in compliance with the principles laid down in Articles 5 and 25 GDPR;
- the Whistleblower receives, before sending the Report, a notice pursuant to Article 13 GDPR specifying the purposes and methods of the processing of his/her personal data and the period of retention thereof, the categories of recipients to whom the data may be transmitted in the context of the management of the Report and the rights recognised to the Whistleblower by the GDPR; the Reported Person is also provided with a notice pursuant to Article 14 GDPR in accordance with the obligations of secrecy and confidentiality imposed by Legislative Decree No. 231/2001, as amended by Law No. 179/2017, as well as in view of the risk of making it impossible or seriously prejudicing the achievement of the purposes of the processing related to the reports under the whistleblowing system (see Article 14(5)(b) and (d) of the GDPR);
- as indicated in the privacy policies provided to data subjects, personal data are processed for the time necessary to achieve the purposes justifying their collection and processing (e.g. evaluation and management of the Report) and subsequently deleted or anonymised according to the defined retention periods;
- appropriate technical and organisational measures are put in place to ensure the security

of personal data, in accordance with the legislation in force, both during the transmission of the Report and during the analysis, management and archiving of the Report;

- the exercise of the rights by the Whistleblower or the Reported Person (the “data subjects” within the meaning of the privacy legislation), in relation to their personal data processed within the Whistleblowing process, may be limited, pursuant to and for the purposes of Article 2-undecies of Legislative Decree 196/2003 as amended by Legislative Decree 101/2018, in the event that an actual and concrete prejudice to other interests protected by specific regulatory provisions may result from such0 exercise, with the clarification that under no circumstances may the Reported Person be allowed to make use of his/her rights to obtain information on the identity of the Whistleblower;
- access to personal data is granted only to persons authorised to receive Reports, limiting the disclosure of confidential information and personal data to third parties only when necessary.

STORAGE OF DOCUMENTATION

In order to ensure the reconstruction of the different stages of the process, the Committee shall ensure:

1. the traceability of Reports and the related receipt, filing, investigation and assessment activities by means of a log system integrated into the digital platform, which keeps track of the date and method of receipt of the report, its type and the results of the investigation;
2. the storage of the documentation relating to the Reports and the related verification activities, as well as any decision-making measures taken by the competent functions, in appropriate files and with the appropriate levels of security/confidentiality;
3. the retention of the documents and Reports for the period of time prescribed by law and in any case no longer than five years from the date of the communication of the final outcome of the reporting procedure.

The functions involved in the activities of verifying the validity of the Report ensure, each to the extent of its competence, the traceability of the data and information and ensure the storage and archiving of the documentation produced so as to allow the reconstruction of the different stages of the process and in accordance with the Group's rules on the storage of documented information.

CONDITIONS FOR EXTERNAL REPORTING

Whereas, as illustrated in this Policy, the Company has set up appropriate internal reporting channels, in compliance with the provisions of Legislative Decree 24/2023, reporting is allowed through the external channel activated by the National Anticorruption Authority ("ANAC"), only in the event that the Whistleblower has:

a) already made an internal report and it was not followed up;

b) reasonable grounds to believe that, if it were to make an internal report, it would not be effectively followed up, or that the report itself might give rise to the risk of retaliation;

c) reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest.

In the absence of the above prerequisites, the report is not handled by ANAC and the person does not benefit from the protections provided for in Legislative Decree 24/2023.

The external reporting channel activated by ANAC is available at the following link: https://whistleblowing.anticorruzione.it/#/.

FUNCTION RESPONSIBLE FOR UPDATING THE POLICY

The Function responsible for this Policy is the Compliance & Safety Function, which updates it periodically, annually or upon specific events to incorporate any organisational and/or regulatory changes.

DISSEMINATION AND COMMUNICATION OF THE POLICY

The Company shall inform all Recipients of the Policy of its existence and content by publishing it on the Sisal Intranet and website.

TRAINING

The Human Resources Function, upon input from or in consultation with the Compliance & Safety Function, is responsible for planning and delivering training activities relating to the Policy and for ensuring its availability and communication.

APPENDIX A – SCOPE OF THE ALERTS

The Report may concern:

- actual or suspected violations of applicable laws or regulations, e.g. employee rights, licensing requirements, etc;
- actual or suspected violations of Sisal, Division and/or Flutter policies;
- conduct that is a criminal offence or constitutes a civil, administrative or accounting violation;
- violations involving legal representatives, directors, managers and/or employees of the Company [or subsidiaries, non-controlled companies in which the Company holds significant shareholdings], joint ventures or - in any case - anyone acting on behalf of the Company (e.g. consultants, suppliers, etc.);
- conduct involving potential conflicts of interest;
- violations relating to the circumvention of Sisal's, Flutter's and/or the International Division's internal accounting controls or policies; including but not limited to:
  - fraud or deliberate error in the preparation, evaluation, review, audit or reporting of any financial statements and/or reports of the Company, the Division and/or Flutter;
  - fraud or intentional errors in the recording and storage of the Company's, Division's and/or Flutter's financial records;
  - deficiencies or non-compliance with the internal accounting controls of the Company, the Division and/or Flutter;
  - non-compliance with legislation or tax obligations.
  - incorrect, incomplete or false statements regarding the financial statements

and/or contained in the financial records, financial reports, audit reports or risk reports of the Company, the Division and/or Flutter; or

- issues affecting the independence of the auditors of the Company, the Division and/or Flutter;
- falsification, concealment or destruction of corporate or financial documents of the Company, the Division and/or Flutter;

- actual or suspected violations of anti-bribery laws or the Company's, Division's and/or Flutter's anti-bribery and corruption Policies, including actual or perceived violations of the rules relating to the provision and receipt of gifts and hospitality;
- potential or actual non-compliance with anti-money laundering and anti-terrorist financing ("AML/CFT") regulations and all related policies and procedures of the Company, the Division and/or Flutter;
- alleged retaliation against a Whistleblower belonging to Company, Division and/or Flutter personnel who has reported a reportable issue under this Policy;
- issues involving a significant threat to the health and safety of Company, Division and/or Flutter personnel and/or the public (e.g. threats of physical violence, harassment, discrimination, bullying, hostile environment, offensive behaviour or drugs abuse impacting the workplace);
- conduct likely to damage the Company's assets or image (e.g. fraud, misappropriation of assets or manipulation of games/products or internal systems to gain an undue benefit or advantage);
- damage to Flutter's property, e.g. by intentionally causing damage or through gross negligence;
- theft, including theft of equipment or of employees' money or personal belongings;
- any issue that may receive negative media or public attention;

- issues that may be deemed significant or sensitive for other reasons, such as a cybersecurity risk or incident;
- any other situation of concern that has been communicated to staff as part of awareness programmes.

APPENDIX B - DISCRIMINATORY MEASURES

The following may constitute discriminatory measures:

- dismissal, suspension or equivalent measures;
- relegation in seniority or non-promotion;
- change of duties, demotion, change of workplace, reduction of salary, change of working hours;
- the suspension of training;
- demerits or negative references;
- the imposition or administration of disciplinary measures, reprimand or other sanction, including a fine;
- coercion, intimidation, harassment or ostracism;
- discrimination, unfavourable or unfair treatment;
- the failure to convert a fixed-term employment contract into a permanent employment contract where the employee had legitimate expectations of being offered permanent employment;
- non-renewal or early termination of a fixed-term employment contract;
- damage, including to the person's reputation, particularly on social media, or financial loss, including loss of economic opportunities and loss of income;
- blacklisting on the basis of a formal or informal sectoral or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future;
- early termination or cancellation of the contract for goods or services;
- cancellation of a licence or permit;

- submission to psychiatric or medical examinations.

APPENDIX C - SAFEGUARDS

The safeguards provided for the Whistleblower in § GENERAL PRINCIPLES also apply to:

a) facilitators (i.e. those who assist the Whistleblower in the Reporting process);

b) third parties connected with the Whistleblower and who might risk retaliation in a work context, such as colleagues or relatives of the Whistleblower;

c) legal entities that the Whistleblower owns, works for or is otherwise connected to in a work context;

d) anyone who has lawfully sought advice in connection with the sharing of information in its possession, has expressed an intention to provide such information, or has provided information or assistance regarding any conduct that might reasonably be expected to constitute a violation of financial, anti-corruption or anti-fraud laws;

e) anyone who has cooperated, filed, caused to be filed, testified, participated or otherwise provided assistance in connection with an investigation or proceeding concerning a financial, anti-corruption or anti-fraud violation of law, or has expressed an intention to do so;

f) anyone who has provided law enforcement agencies with truthful information about the possible or actual commission of a criminal offence or other violation of law, unless such persons are the perpetrators of such violations; or

g) anyone who has cooperated, participated or provided assistance in the investigation phases of the reports to the persons designated to do so.

Moreover, the above protections also apply if the report is made:

(i) when the employment relationship has not yet commenced if information on violations was acquired during the selection process or at other pre-contractual stages;

(ii) during the probationary period; or

(iii) after the termination of the legal relationship, if the information on violations was acquired in the course of that relationship.