WHISTLEBLOWING POLICY

Reply Group

CONTENTS

1 REPLY GROUP PREVENTS MALPRACTICE

The group controlled by Reply S.p.A. (hereinafter also referred to as "**Reply**" and, together with its subsidiaries, the "**Reply Group**" or the "**Group**") is engaged in the field of Information & Communication Technology at worldwide level, through a network of companies specialized by business line, which rely on accurately recruited and well-trained professionals, with a focus on the quality of service and client satisfaction.
Success in the business world increasingly depends on companies understanding and living up to market expectations in terms of ethical standards which are constantly pursued by Reply Group through, among others, its set of procedures and the relevant Code of Ethics adopted by the Group (https://www.reply.com/InvestorsDocuments/en/Code_of_Ethics.pdf).
Reply Group – also in light of a responsibility to its investors – has the duty to identify and take measures to remedy all malpractices detected within the organization; in this context, Reply Group encourages a culture of openness within the organization, to increase its ability to prevent malpractice.

2 PURPOSE OF THE WHISTLEBLOWING POLICY

The purpose of this Policy (hereinafter the "**Policy**") is to provide, in compliance with the applicable laws, a framework to promote responsible and secure whistle blowing; in particular, the Policy is aimed to:

- encourage personnel to report suspected (but grounded) wrongdoing as soon as possible in order to allow to investigate, as appropriate, such wrongdoing;
- reassure personnel that they should be able to raise genuine concern without any reprisal affecting their work.

"Malpractice" or "wrongdoing" for the purpose of this Policy refers to actions which may be:

i) illegal in accordance with the applicable laws, improper, or unethical;
ii) in breach of a professional code and/or Reply Group policies;
iii) acts which are otherwise inconsistent with the Code of Ethics of Reply Group; and, more in general
iv) any act or omission which may cause any type of harm (e.g. economic, environmental, to safety of workers or of third parties, or merely reputational) to the Reply Group companies and their customers, shareholders, partners, third parties and, more generally, to the community.

It remains understood that the enforceability and effectiveness of this Policy does not affect / amend the obligations to submit reports/claims to the competent judicial, supervisory or regulatory authorities in the countries where Reply Group companies perform their business, or the obligations to submit reports to any control bodies established at each Group company.

3 ADDRESSEES

This Policy constitutes the reference document for all companies belonging to the Reply Group, without detriment to any mandatory provision required by each specific local law regulating the same subject which will automatically finds its application.

The addressees of this Policy ("**Addressees**" and/or "**Whistleblowers**") are the:

a) boards' components of all companies belonging to the Reply Group;
b) each Reply Group employee;
c) consultants,
d) shareholders and, more generally, the stakeholders of the Group.

4 REPORTS

Addressees who discover or otherwise become aware of possible malpractice committed by parties who have relations with one or more companies belonging to the Reply Group during their working activities or that have an

impact on these working activities, must activate this Policy by reporting the actions, events and circumstances that they believe, in good faith, have caused violations and/or actions contrary to the Group's principles ("**Report**").
If an Addressee is concerned about any form of malpractice, he/she should normally first raise the issue with the reference persons having direct knowledge of the issue. There is no special procedure for doing this - simply tell them about the problem or put it in writing if preferred.
Should this not be possible, for whatever reason, the Addressee should draft a proper Report which shall include:

- a detailed description of the events that occurred and how the Whistleblower becomes aware of them;
- the date and place of the event;
- the names of the persons involved, or information that enables their identification;
- the names of any other parties who can attest to the actions set out in the Report;
- reference to any documents that could confirm that the reported actions did occur.

The Whistleblower must put his/her name to allegations. Concerns expressed anonymously will not be investigated.
The Report so completed should be then sent:

- by email, to the email address: odv@reply.com – accessible only to the members of the Supervisory Body of Reply S.p.A.;
- by post, to: Reply S.p.A. – Via Nizza n.250 – 10126 Turin - Italy, for the attention of the Supervisory Body of Reply S.p.A..

During the checks on the validity of the Report received, the sender may be contacted by the Supervisory Body to request any additional information that may be required.

5 CONFIDENTIALITY

Reply Group guarantees the confidentiality of the Report and the information it contains, as well as the anonymity of the Whistleblower, in compliance with the laws in force and the requests of the judicial authority.
Any kind of threat, retaliation, penalty or discrimination against the Whistleblower or the reported party – or anyone who has participated in the investigation into the validity of the Report – will not be tolerated.
Reply Group reserves the right to take the appropriate actions against anyone who retaliates or threatens to retaliate against Whistleblowers who have submitted Reports in accordance with this Policy, without detriment to the right of the affected parties to seek legal protection if the Whistleblower is found to be criminally or civilly liable for falsehoods in their statements or reports.
Reply Group may take appropriate disciplinary and/or legal measures to protect its rights, assets and reputation against anyone who, with gross negligence or willful misconduct, has made false, unfounded or opportunistic Reports and/or has made Reports for the sole purpose of defaming, slandering, or causing harm to the Reported Party or to other parties mentioned in the Report.

6 CHECKS ON THE VALIDITY OF THE REPORT

The Supervisory Body is responsible for checking the validity of the Report on behalf of the entire Reply Group, without prejudice to any specific local laws on the subject. As such it will perform a prompt and thorough investigation, in observance of the principles of impartiality, fairness and confidentiality towards all parties involved.
During the course of these checks, the Supervisory Body may request assistance from the company departments competent in each instance. Where appropriate, the Supervisory Body may also request the assistance of external consultants specialized in the area of the Report, provided their involvement is conducive to verifying the Report and ensuring its confidentiality.
Once the checking phase has been completed, the Supervisory Body will prepare a summary report on the investigations carried out and the evidence that it has considered, and the report will be shared with the Board of Directors of Reply S.p.A., so that they can draw up intervention plans and decide what action to take to protect the Reply Group.
If the investigations conclude that there is insufficient evidence or that the events referred to in the Report are unproven, the Report will be archived.
The Supervisory Body periodically reports on the types of reports received and on the results of its investigative activities to the Board of Directors.

7 PROCESSING OF PERSONAL DATA

The personal data of Whistleblowers and of any other parties involved that is obtained while handling the Reports (including any sensitive data, such as racial and ethnic background, religious and philosophical beliefs, political opinions, membership in political parties or trade unions, and personal data indicative of a person's health and sexual orientation) will be processed in full compliance with the provisions of current legislation regarding the protection of personal data, with the policies and the processes of the Reply Group.

Legitimate interest is the basis for lawful processing.

In the management of the report, in accordance with the requirements of the GDPR, a balance of interests will be held, protecting the identity of the whistleblower, and providing the affected parties with the possibility to verify the contents of the accusations in order to defend themselves in compliance with their personal rights.

Only the data strictly necessary for verifying the validity of the Report and for handling it will be processed. Therefore, to ensure proper management of the Reports received and to comply with legal or regulatory obligations, irrelevant personal data obtained will be deleted.

During the checks on the validity of the Report the relevant personal data will be communicated exclusively to the persons and bodies relevant for the necessary activities. In addition, appropriate measures will be taken to protect personal data from unauthorized access, unauthorized changes, even partial destruction and unauthorized disclosure, in order to prevent harms to the persons concerned.

The Supervisory Body may disclose the personal data contained in the Reports to company boards and to the internal departments competent in each instance, as well as to the judicial authorities, in order to start the procedures necessary for guaranteeing proper legal and/or disciplinary action against the Reported Party/Parties, provided that the information collected and the checks carried out show that the contents of the Report are true. In these cases, the personal data may also be disclosed to external parties specialized and authorized.

All necessary measures will be taken to protect the data from accidental or unlawful destruction, loss or unauthorized disclosure during the activities to verify the validity of the Report. Furthermore, the documents regarding the Report shall be preserved in both paper copy and digital format for a period of time no longer than strictly necessary for the proper completion of the procedures established in this Policy.

Copies of superfluous data will be avoided on email attachments, on PCs, on cloud services or elsewhere to facilitate access control, protection and removal of data.