WHISTLEBLOWING POLICY AND PRIVACY NOTICE

Reply Group

CONTENTS

1 PREVENTION OF MALPRACTICE IN THE REPLY GROUP 3
2 PURPOSE OF THE WHISTLEBLOWING POLICY 3
3 ADDRESSEES AND WHISTLEBLOWERS 3
4 INTERNAL AND EXTERNAL REPORTS 3
5 CONFIDENTIALITY 4
6 ASSESSMENT ON THE REPORT 4
7 PROCESSING OF PERSONAL DATA 5
ANNEX I – FRANCE 7
ANNEX II – GERMANY 8

1 PREVENTION OF MALPRACTICE IN THE REPLY GROUP

The Reply Group is engaged in the field of Information & Communication Technology at worldwide level, through a network of companies specialized for business lines, which rely on accurately recruited and well-trained professionals, with a focus on the quality of service and client satisfaction.
The Reply Group operates by constantly pursuing high ethical standards, as defined in its Code of Ethics (https://www.reply.com/contents/Code_of_Ethics.pdf).
The Reply Group, also in light of its responsibility towards its investors, has the task of identifying and adopting measures aimed at remedying all unlawful conduct detected within the organization; in this context, the Reply Group encourages a culture of openness within the organization itself to increase its ability to prevent and/or counter such unfair practices.

2 PURPOSE OF THE WHISTLEBLOWING POLICY

The purpose of this Whistleblowing Policy is to provide, in compliance with the applicable laws, a framework to promote responsible and secure whistleblowing; in particular, the Whistleblowing Policy is aimed at:

- encouraging personnel to report suspected (but evidenced) malpractice or wrongdoing as soon as possible in order to allow the relevant functions to carry out the necessary investigations;
- reassuring personnel that they are able to raise genuine concern without any reprisal affecting their work.

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

i) illegal acts in accordance with the applicable laws, or improper or unethical acts;
ii) acts 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, related to human rights, 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.

This Whistleblowing Policy does not affect or amend the obligations to submit reports or 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 supervisory bodies established at each Group company.

3 ADDRESSEES AND WHISTLEBLOWERS

The **Addressees** of this Whistleblowing Policy are the:

i) board members of all companies belonging to the Reply Group;
ii) all employees of the Reply Group companies, collaborators, partners, suppliers, customers and, more generally, anyone who has a relationship with any of the Reply Group companies.

The Addressees who make a Report on the basis of the information acquired in the context of their working context are identified as the **Whistleblowers**.

4 INTERNAL AND EXTERNAL 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 while performing their working activities or that have an impact on these latter, must activate this Policy by reporting the actions, events and circumstances that they believe, in good faith, have caused breaches and/or actions contrary to the Reply Group's principles ("**Report**") to the Supervisory Body appointed by the Reply Group with the goal of managing such Report.

If an Addressee is concerned about any form of malpractice, he/she should draft a Report (based on precise and consistent evidence) which shall include, for instance:

- a detailed description of the event(s) that occurred and how the Whistleblower became aware of them;
- the date and place of the event(s);
- the personal data of the persons involved, or other elements or information enabling their identification;
- the personal data 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;

- any other information that can evidence the facts subject to the Report.

The Report so completed should be then sent:
- online, by*:* https://reply-whistleblowing.integrityline.com/?lang=en ;
- by mail: to Reply S.p.A. – Via Nizza n.250 – 10126 Turin - Italy, for the attention of the Supervisory Body;
- by phone: to +390117711594, asking for the Supervisory Body.

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

The following Reports will not be taken into consideration for the purposes of carrying out the preliminary investigation, except for any requests for additions or forwarding to the competent bodies:
a) pertaining to facts which do not relate either to the personnel or to the scope of Reply or the Group;
b) exclusively concerning disputes, claims or requests related to a personal interest of the Whistleblower only pertaining to his or her individual work relationships or inherent in his or her work relationships with hierarchically higher figures;
c) based on mere suspicions or rumors.

5 CONFIDENTIALITY

Reply Group guarantees the confidentiality of the Report and the information contained therein, as well as the anonymity of the Whistleblower, in compliance with the laws in force and the requests of the judicial authority. All information received with the Report will be treated confidentially by the Supervisory Body.

Any kind of threat, retaliation, penalty or discrimination against the Whistleblower or the reported party – or anyone who has participated in the investigation related to the Report – will not be tolerated (*e.g.* dismissal, downgrading or non-promotion, change of duties and/or place of work, reduction of salary, change in working hours, adoption of disciplinary measures or other sanctions, including pecuniary ones, penalization in the qualification of the supplier or the non-renewal without justified reason).

Reply Group reserves the right to take the appropriate action against anyone who retaliates or threatens to retaliate against Whistleblowers who have submitted Reports in accordance with this Whistleblowing Policy, without detriment to the right of the affected parties to seek for 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 or unfounded Reports and/or has made Reports for the sole purpose of defaming, slandering, or causing harm to the Whistleblower or to other parties mentioned in the Report.

6 ASSESSMENT ON THE REPORT

The Supervisory Body is responsible for checking the validity and truthfulness of the Report on behalf of the entire Reply Group, without prejudice to any specific local laws on the relevant topic. As such it will perform a prompt and thorough investigation, in compliance with the principles of impartiality, fairness and confidentiality towards all parties involved.

The Supervisory Body, in accordance with the provisions of the relevant legislation, shall issue to the Addressee an acknowledgement of receipt of the Report within 7 (seven) days from the date of receipt.

All Reports are subject to preliminary analysis by the Supervisory Body in order to verify that data and information are useful to allow an initial assessment of the Reports as well as their compliance with the requirements of the relevant legislation. To this end, the Supervisory Body, if deemed necessary, may request the Addressee to provide any additional information concerning the Report.

At the end of these preliminary checks, in the event of unfoundedness or inaccuracy of the facts referred to in the Report, or when the Report has become irrelevant, the Supervisory Body shall proceed with the filing of the Report, giving written notice to the recipient.

While carrying out these checks, the Supervisory Body may request assistance from the competent corporate departments or, where appropriate, from external consultants specialized in the matter of the Report, provided their involvement is functional to verifying the Report and ensuring its confidentiality.

The Supervisory Body shall provide feedback to the Addressee on the Report within a reasonable period not exceeding 3 (three) months after acknowledgement of receipt of the Report or, in the absence of such notice, 3 (three) months after the expiry of a period of 7 (seven) working days from the Report's submission.

Once the investigation 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 the companies to which the Addressee belongs to and to the Board of Directors of Reply S.p.A., so that they can draw up any intervention plans and decide the actions to be taken to protect the Reply Group's interest, as well as taking the appropriate decisions regarding any actions against the reported subject (in case of validity of the Report) or the Whistleblower (in case of Report made with willful misconduct or gross negligence); in cases of evidenced reports of illegal act and/or involving reports to the Authorities, the Supervisory Boards are informed.

The Supervisory Body periodically reports on the types of Reports received and on the results of its investigative activities to the Board of Directors of the companied involved and, if necessary, to the Board of Directors of Reply S.p.A..

7 PROCESSING OF PERSONAL DATA

Reply S.p.A. with registered office in Corso Francia n. 110, Turin, Italy, ("Reply" or "Owner"), as data controller, provides below the information on the processing of personal data of the subjects involved in the process of receiving and managing Reports of alleged offences.
Reports can be made via EQS Integrity Line, an online communication system of EQS Group (EQS Group AG, Hardturmstrasse 11, 8005 Zürich, Switzerland).

As part of the management of Whistleblowing, the personal data being processed are the data of the Whistleblower, the "Reported" and any other third parties such as the persons involved, mentioned and/or connected to the facts covered by the Whistleblowing ("Data Subjects").
The receipt and management of Reports may give rise to the ordinary personal data processing (e.g. name, surname, job role), as well as, depending on the content of the Reports and the deeds and documents attached to them, may give rise to the particular personal data processing (data relating to health conditions, sexual orientation or trade union membership) and personal data relating to criminal convictions and crimes.
The data can be collected both directly from the interested party and through other subjects involved in the Report.

The provision of the whistleblower's personal data is not mandatory in the Report*, as it is possible to make a Report anonymously through the EQS integrity Line.*

Personal data is processed exclusively for the purpose of ensuring:
(i) the correct and complete management of the Report in compliance with current legislation on whistleblowing;
(ii) the necessary preliminary activities aimed at verifying the validity of the subject matter of the Report and the adoption of the consequent disciplinary and/or judicial actions against those responsible for the unlawful conduct;
(iii) the protection in court of a right of the Data Controller and/or of a company of the Reply Group;
(iv) the response to a request from the Judicial Authority or similar Authorities.

The legal basis for processing of point i), ii) and iv) is represented by the fulfillment of legal obligations to which the Data Controller is subject with reference to the provisions contained in laws; the legal basis for processing iii) is represented by the legitimate interest of the Data Controller and/or of a company of the Reply Group.

In particular, the personal data collected are only those necessary and relevant for the achievement of the purposes indicated above, on the basis of the "principle of minimization". With respect to these data, the interested party is requested to provide only the data necessary to describe the facts covered by the Report without communicating

redundant personal data or data other than those necessary with respect to the purposes indicated above. If provided, such data will be deleted.

Where it is necessary to process personal data that requires the consent of the interested party, the latter will be invited to provide it to the personnel authorized to manage the Report.

During the Report management activities, specific security measures will be adopted to prevent data loss, illicit or incorrect use and unauthorized access, modification and/or disclosure. All those who receive and/or are involved in the management of the Reports are required to protect the confidentiality of such information. It should be noted that the identity of the Reporter will be protected upon receipt of the report and in each subsequent phase, as indicated in paragraph 5 of this Whistleblowing Policy.

The documents relating to the Report will be kept both in hard copy and in digital format for a period of time not exceeding what is strictly necessary for the correct finalization of the procedures established in this Policy, and in any case no later than 5 (five) years from the date of the communication of the final outcome of the Reporting procedure, in accordance with the provisions of the relevant legislation.
With a view to facilitating access control, data protection and removal, unnecessary copies of the data will not be made on e-mail attachments, PCs, cloud services, etc...

The communication of the pertinent personal data collected is made exclusively to recipients and/or competent bodies whose activity is necessary for the performance of the activities related to the management of the Report. The Supervisory Body may communicate the personal data contained in the Reports to the Boards of Directors of the Italian companies of the Reply Group and to the competent internal functions, as well as to the Judicial Authorities, in order to initiate the procedures necessary to guarantee suitable judicial protection and /or disciplinary measures against the reported subjects, where the validity of the circumstances initially reported emerges from the elements collected and from the checks carried out; moreover, the data may also be communicated to specialized and authorized external subjects.

Interested parties have the possibility to exercise specific rights; for example, under certain conditions, interested parties can exercise the right of access, rectification, cancellation, limitation of treatment. Interested parties also have the right to object, for reasons connected to particular situations, to the processing of their personal data based on legitimate interest, save for the existence of legitimate reasons.

The exercise of these rights is subject to some exceptions aimed at safeguarding the public interest (for example, the prevention or identification of crimes) and the interests of Reply (for example, the maintenance of professional secrecy).
These rights can be exercised with a request addressed to: odv@reply.com .

The interested party may also contact the Personal Data Protection Authority.

In the event that some personal data have been processed with the consent of the interested party, the latter has the right to revoke this consent at any time, but without affecting the lawfulness of the processing, based on consent, carried out before the revocation.

The contact details of the Data Protection Officers and Privacy Representatives are:

- DPO Italy: dpo.it@reply.it
- DPO Germany: dpo.de@reply.de
- DPO UK: dpo.uk@reply.com
- Brazil: privacy.security.br@reply.com
- USA: privacy.security.us@reply.com

ANNEX I – FRANCE

The Addressee is also guaranteed with the possibility to make an external Report, either after making an internal Report (which does not prove to be effective) or directly, to one of the following authorities:

- one of the competent authorities listed in Annex I of the "*Décret n° 2022-1284 du 3 octobre 2022 relatif aux procédures de recueil et de traitement des signalements émis par les lanceurs d'alerte et fixant la liste des autorités externes instituées par la loi n° 2022-401 du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte*";
- the so-called "Rights Advocate", who in turn forwards the Report to the competent authority for the relevant processing procedures;
- judicial authority;
- an institution, body, or agency of the European Union competent to collect information on violations within the scope of EU "*Directive no. 2019/1937 of the European Parliament and the Council of 23 October 2019 on the protection of persons who report breaches of Union law*".

The external reporting channel ensures the integrity and confidentiality of the information contained in the Report, with particular reference to the identity of the Addressee, the person(s) involved in the Report and any third parties mentioned therein.

External Reports can be made in writing or in oral form (by phone or any other voice mail system) or, at the Addressee's request, through physical meetings or videoconference no later than 20 (twenty) working days from the date of receipt of the relevant request.

When submitting the Report, the Addressee must specify whether or not he/she has made prior use of the internal reporting channel.

The competent authority shall issue to the Addressee an acknowledgement of receipt of the Report within 7 (seven) days from the date of receipt (unless expressly waived by the Addressee or unless the competent authority considers that the relevant issuance would compromise the protection of the confidentiality of the Whistleblower's identity), and shall provide feedback to the Addressee on the measures (taken or to be) taken to assess the accuracy of the allegations and, if necessary, to remedy the object of the Report, as well as on the reasons justifying the adoption of such measures, within a reasonable period not exceeding 3 (three) months after acknowledgement of receipt of the Report or, in the absence of such notice, 3 (three) months after the expiry of a period of 7 (seven) working days from the Report's submission. Such period may be extended to 6 (six) months in the presence of specific circumstances that require further actions, in which case the competent authority shall justify such circumstances to the Recipient before the expiry of the aforementioned 3 (three) month period.

The competent authority files the Report when this latter has become irrelevant or when the allegations are inaccurate, unfounded or contain no significant new information compared to a Report which has already been filed. The Addressee shall be informed in writing of the Report's closure as well as of the relevant reasons.

ANNEX II – GERMANY

Reports can be made in writing or in oral form (by phone or any other voice mail system) or, at the Addressee's request, through physical meetings or videoconference within a reasonable period of time from the date of receipt of the relevant request. Reports received anonymously are also processed.

The Addressee is also guaranteed with the possibility to make an external Report, either after making an internal Report (which does not prove to be effective) or directly, to one of the following authorities:

- Federal Office of Justice (Bundesamt für Justiz (BfJ));
- Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin));
- Federal Cartel Office (Bundeskartellamt);
- an institution, body, or agency of the European Union competent to collect information on violations within the scope of EU "Directive no. 2019/1937 of the European Parliament and the Council of 23 October 2019 on the protection of persons who report breaches of Union law".

The external reporting channel ensures the integrity and confidentiality of the information contained in the Report, with particular reference to the identity of the Addressee, the person(s) involved in the Report and any third parties mentioned therein.

When submitting the Report, the Addressee must specify whether or not he/she has made prior use of the internal reporting channel.

For both internal and external Reports the following applies:

The Addressee shall receive confirmation within 7 days that the Report has been received (unless expressly waived by the Addressee or unless the competent authority considers that the relevant issuance would compromise the protection of the confidentiality of the Whistleblower's identity). Within 3 months at the latest after confirmation of receipt of the Report, Addressee shall be informed of any follow-up measures planned or already taken, as well as the reasons for them. The Report will be file when this latter has become irrelevant or when the allegations are inaccurate, unfounded or contain no significant new information compared to a Report which has already been filed. The Addressee shall be informed in writing of the Report's closure as well as of the relevant reasons.

Incoming reports will be documented in accordance with confidentiality obligations of Section 5. The documentations are deleted 3 years after the conclusion of the procedure. In exceptional cases, documentation may be kept for longer than 3 years to meet requirements under the German Whistleblower Protection Act (Hinweisgeberschutzgesetz) or other legislation, as long as this is necessary and proportionate.

GERMAN SUPPLY CHAIN ACT (LKSG)

The regulations of the Whistleblowing Policy set out above apply to the same extent to reports of violations of human and environmental rights under the German Supply Chain Act (LkSG).

Our Human Rights Officer will be informed if there is a report of existing or potential human or environmental rights violations. Documentations are deleted 7 years after the conclusion of the procedure.