Amplifon S.p.A.

Group Whistleblowing Policy

Release 2021

Contents

1 Introduction

Amplifon's commitment

Amplifon carries out its business correctly, transparently, honestly, faithfully and lawfully and requires all the Group's companies, executives, members of management, employees and stakeholders to abide by those laws, regulations, rules of conduct, standards and guidelines, both national and international, which apply to the Group's companies. Whistleblowing is of paramount importance for Amplifon in reinforcing control over the effective application of and compliance with the Code of Ethics as well as the provisions and principles of the Policies and Procedures. Moreover, a *whistleblowing* system, in line with international and local laws and *best practice*, helps Amplifon to strengthen business integrity and effectively tackle potential issues at an early stage, reducing the risk of significant possible damage to the Group's business and reputation.

For this reason, Amplifon greatly encourages and recommends taking notice of the breach of these principles and the Company takes any possible whistleblowing report as identified in this Policy extremely seriously. *(Please refer to the specific Section "2. What to report").*

To this end, also the Digital Whistleblowing System, described in this Policy, has been implemented within the Group; its design is based on the highest international standards, using the best available digital technologies.

The Group ensures that the confidentiality of the reports received is protected to the maximum extent possible under the applicable law and also guarantees that no person within Amplifon may be dismissed, demoted, suspended, threatened, harassed, subject to retaliation or discriminated against in any way with respect to their working conditions for having submitted a report pursuant to this Policy.

Similarly, no person within Amplifon will be penalized for reporting possible violations which are then found to be unsubstantiated if there was a reasonable belief to justify reporting them.

Group Whistleblowing Policy

This document contains a description of the reporting process and the related management, as well as the indication of the rights and obligations concerning Whistleblowers; it applies to all Amplifon's companies in all geographic areas where the Group operates and must be interpreted and applied in each relevant country consistently and in compliance with any specific local laws on the same subject.

Any particular regulatory aspects of each country may be the subject of specific annexes/additions to this Policy, drafted by the Group's companies, in coordination with the Whistleblowing Committee.

The principles of this Policy do not affect - and do not in any way limit - the obligations to submit reports to the competent judicial, supervisory or regulatory authorities in the countries where entities belonging to the Group operate, or the obligations to submit reports to any control bodies established at each Group's company.

This Policy, approved by the Board of Directors of Amplifon S.p.A. on March 04, 2020, has been subsequently updated on a periodic basis in order to incorporate regulatory changes and organizational variations in line with the reference *best practices*. Its application is mandatory for all companies belonging to the Group.

Each of Amplifon's companies (including the companies that are established/become part of the Group) will adopt this Policy (and any new version of the same) through a resolution of its Board of Directors (or

of the corresponding body/department/role if the governance of the respective company does not provide for such body) during the first possible meeting and in any case no later than 60 working days from the date provided for in the action plan defined at Group level.

When required by local legislation, the relevant company of the Group will ensure that this Policy (and any new version of the same) will be duly submitted to the authorization or approval of the competent authorities or local bodies.

2 What to report

Whistleblowing channels serve the purpose of transmitting the reports of actual or suspected breaches of which the recipients of this Policy reasonably suspect concerning conducts (of any nature whatsoever, even if merely omissive) in violation of:

(i) the Group's Code of Ethics;
(ii) the laws applicable to each Group's company;
(iii) the regulations or measures issued by any competent Authority; and/or
(iv) the internal policies and procedures adopted by the Group's companies (e.g., conflicts of interest, anticorruption, etc.).

The foregoing is implemented within the Digital Whistleblowing System settings, without prejudice to the different provisions under local legislation to the different countries (e.g., Italy: Model 231).

In some countries, local laws and regulations restrict reports of situations, information or documents which are covered by secrecy or legal privilege in certain circumstances. If you are not sure whether the laws or regulations on documents covered by secrecy or concerning confidential information apply to a report, then we recommend speaking with the subjects mentioned under Section 9.

Unless a different definition of Third Parties is provided for by applicable local laws, for the purposes of this Policy, Third Party(ies) means any external party with whom the company of the Group has some form of business relationship (e.g., joint ventures, joint venture partners, consortium partners, outsourcing service providers, contractors, consultants, sub-contractors, suppliers, vendors, advisors, agents, distributors, representatives, intermediaries and investors).

Reports must be made based upon reasonable belief and must be as detailed as possible. They must contain information and facts rather than allegations or statement of opinions, without prejudice to any specific additional requirements provided for by applicable local laws.

No reports concerning personal grievances and customer experience, or product complaints can be accepted under this Policy.

3 Roles and Responsibilities

- **Whistleblower Protection Officer:** the Group Internal Audit and Risk Management Officer has the task of receiving, collecting and preliminarily analyzing reports submitted by Whistleblowers and calling for the Whistleblowing Committee meeting.
- **Whistleblowing Committee:** the Whistleblowing Committee, appointed by the Board of Directors of Amplifon S.p.A., is composed of (i) the Chief HR Officer, (ii) the Chief Legal Officer and (iii) the Group Internal Audit and Risk Management Officer, and is engaged to investigate and report to the Control, Risk and Sustainability Committee, reports that are received through Whistleblowing channels and to define the related disciplinary measures.

- "**Whistleblower**": the person responsible for submitting whistleblowing reports to Amplifon's administrators, directors, officers, managers, employees as well as the Third Parties[1], according to the case in question.

4 General principles

4.1 Confidentiality

All reports must be dealt with in a confidential manner to the extent possible under local law and in order for Amplifon to investigate a report and take appropriate steps. Amplifon is committed to protecting the Whistleblower's identity and the confidentiality of all the information contained in the reports (including the identity of reported persons) throughout the entire report management process - from the time the reports are received and throughout the investigation and final stages - by all the people involved for any reason whatsoever in the management process, in compliance with applicable local privacy laws and consistently with the needs of the investigation process. Upon filing of his/her report, the Whistleblower is bound to treat it (and the underlying facts and circumstances) with utmost confidentiality, subject to applicable law. The measures to protect the Whistleblower's confidentiality are aimed, among other things, at ensuring that he/she is not subject to any form of retaliation. The violation of this principle may lead to disciplinary proceedings against the author of this violation and the imposition of the related disciplinary measures, in accordance with the provisions of the applicable national labor law legislation.

Moreover, the following measures have been adopted:

- the transmission/storage of the reported information is carried out using the Digital Whistleblowing System; if exceptionally submitted through other channels, the reports must be promptly loaded into the Digital Whistleblowing System and, in any event, the information contained therein must be properly secured;
- the transfer of paper documents should be avoided;
- all stages of the report management process are carried out in a protected electronic environment, accessible only to specifically authorized people, and based on pre-established "access levels";
- throughout all stages of the report management process, the data concerning Whistleblowers are kept strictly confidential to the extent possible under local law and in order for Amplifon to be able to investigate a report and take appropriate steps;
- anyone who is aware that the reported information has reached people not involved in the management process must report this to the Whistleblowing Committee.

Furthermore, the breach of confidentiality and privacy obligations may lead to disciplinary liability, without prejudice to further kinds of liability provided for by the applicable legislation.

4.2 Ban on retaliation

No Whistleblower reporting a breach based on a reasonable belief in accordance with the provisions of the present Policy shall suffer retaliation. Whistleblowers are protected against any retaliatory or discriminatory act, direct or indirect, for reasons connected, directly or indirectly, to the report; in

[1] Third Parties who have access to Amplifon's intranet may submit any reports using the Digital Whistleblowing System. Other Third Parties may use the institutional reporting channels provided on the Amplifon S.p.A. website, or other channels specifically established by the Group's companies, in accordance with applicable local legislation.

particular, no Amplifon's people can be dismissed, demoted, suspended, threatened, harassed or discriminated against in any way in their working conditions for having submitted a report pursuant to this Policy. This protection is guaranteed to the Whistleblowers even when the report, albeit unfounded, is based on a reasonable belief.

Amplifon is greatly committed to safeguarding everyone acting in the interest of protecting its culture and values: therefore, any detrimental action performed against a Whistleblower may be identified as retaliation and may be punished. To implement this principle, rules have been defined in order to ensure the protection of Whistleblowers from any form of retaliation, including through the direct and specific commitment of the company's managers, in the persons of the administrators and top management (known as "Top level commitment"). In this regard, the following is established:

- the availability of the Digital Whistleblowing System - as well as the alternative channels indicated in section 5.1 - for reporting any violation of the non-retaliation principle to the Whistleblowing Committee;
- the duty of the Whistleblowing Committee to promptly and effectively conduct relative investigations, with the support of the competent departments involved in the events reported;
- the duty of the Whistleblowing Committee to verify and assess, without delay, the situations described above and to promptly inform the Group's directors and the top management about the outcomes of that assessment; and
- the traceability and transparency of all information relating to the activities described above.

To this end, the Whistleblowing Committee, with the help of the local HR Department, monitors any retaliation, unfair and discriminatory behaviors towards the Whistleblowers, through the analysis and overall assessment of specific suspect situations ("Red Flags") (e.g.: changes of office or job, transfers of headquarters, requests for job changes, long absence due to illness, disciplinary disputes / measures, requests for unpaid leave, negative performance assessments, etc.).

Finally, any violation of the prohibition to engage in retaliatory and discriminatory behavior may result in disciplinary proceedings being initiated against the individual who engaged in this behavior and the imposition of appropriate disciplinary measures in accordance with existing legislation and applicable national collective work contracts.

All Amplifon's people must be made aware of these rules and procedures to protect employees during the training activities.

4.3 Anonymous reports

Amplifon allows the submission of anonymous reports. However, Amplifon encourages their people not to make complaints anonymously, as "confidential" reports facilitate the interaction with and request for clarification from the Whistleblower, whilst at the same time guaranteeing the Whistleblower the maximum confidentiality and protection available under local law, including against retaliatory and/or defamatory reports.

4.4 Misuse of the Group Whistleblowing Policy

Amplifon welcomes all reports made based on a reasonable belief and in compliance with the provisions of this Policy. Any manifestly unfounded or defamatory report as well as reports not in compliance with this Policy may constitute misconduct, resulting in possible disciplinary measures and potential liabilities for the Whistleblower.

4.5 Duty of independence and professionalism in the management of reports

All parties involved, for whatever reason, in the report management process must perform the related tasks in compliance with the duties of independence and ensuring the accurate and efficient management of all reports.

4.6 Protecting the integrity of reports

Amplifon ensures that no reports (from the notification to the decision phase) are canceled and/or altered notwithstanding the retention provisions specified in Section 6 below.

4.7 Other provisions

The Whistleblower will be protected from any civil, criminal, or administrative liability in relation to the disclosure of the report in compliance with applicable local law provisions. Applicable compensation provisions must also apply.

5 Report management process

The reports are managed in an integrated manner for all the companies belonging to the Group pursuant to the following provisions.

5.1 Reporting channels

Reports must be submitted to the Whistleblowing Committee through the Digital Whistleblowing System - as specifically designed to ensure maximum ease of use for the best protection of Whistleblowers - accessible from any PC, tablet or smartphone.

Whistleblowers may also use the alternative channels indicated below:

- **e-mail** to the following **e-mail address**: wbcommittee@amplifon.com accessible only by the members of the Whistleblowing Committee;
- **ordinary mail** to the attention of one of the members of the Whistleblowing Committee at the following address:

  Amplifon S.p.A.

  Via Ripamonti, 133

  20141 Milano - Italy

In case of reports submitted by using channels other than the Digital Whistleblowing System, in order to take advantage of a greater guarantee of confidentiality, it is necessary that the report is inserted in a closed envelope that bears the wording *"confidential/personal*" or that the subject-matter of the e-mail contains the aforementioned wording.

However, the recommendation to use the Digital Whistleblowing System is renewed, unless for technical reasons it is not possible to access it, since:

i) the use of alternative channels cannot guarantee the same level of protection of the Whistleblowers and efficiency in the management of the reports;
ii) in the case of anonymous reporting, the use of the Digital Whistleblowing System is the only method that allows Amplifon to contact the Whistleblower for further information and

clarification, while maintaining his/her anonymity, based on the methods described in section 5.2 below.

Anyone who receives a report through channels alternative to the Digital Whistleblowing System must promptly deliver it personally or by ordinary mail or express courier, avoiding any e-mail or digital forwarding to the Whistleblower Protection Officer, who will insert the report in the Digital Whistleblowing System, keeping the information received strictly confidential.

5.2 Access to the Digital Whistleblowing System and submission of reports

To access the Digital Whistleblowing System the Whistleblower must access the intranet link: the Whistleblower will be directed to a first screen that allows him/her to (i) submit a report or (ii) check the status of a previous report.

If the Whistleblower selects the "Report" button, a second screen will open where two reporting options will appear: one for Amplifon's employees and one for the Third parties.

If the "Employee" option is selected, the Whistleblower can choose to submit his/her report in confidential way by logging in with Single Sign On - SSO (**confidential report**) access or to report anonymously (**anonymous report**).

Similarly, if the "Third Party" option is selected, the Whistleblower can choose to provide the identification data (**confidential report**) or stay anonymous (**anonymous report**).

In the event of a "confidential" (not anonymous) report, the Whistleblower enters his/her identification data in the appropriate fields (unless the Whistleblower logged in with SSO) on the compilation page of the Digital Whistleblowing System and reports the alleged violation (by filling in all the required fields).

In the event of an "anonymous" report, the Whistleblower is only required to fill in the fields describing the alleged violation; in this case, the fields relating to the whistleblowers' identification data are not provided on the compilation page.

The Digital Whistleblowing System settings also allow the Whistleblower to select the company of the Group to which the report refers and to specify the subject-matter of the violation by selecting it from a pre-set list proposed by the Digital Whistleblowing System.

The report must:

- contain a precise description of the facts and the persons involved, to the extent possible;
- be integrated by attaching any documentation supporting the alleged violation to the extent possible, using the appropriate document upload function made available by the Digital Whistleblowing System.

Upon receipt of the confidential report, the Digital Whistleblowing System anonymizes the Whistleblower's data automatically inserting them in a separate archive accessible exclusively to the members of the Whistleblower Committee and only for the reasons laid down within the applicable legislation. Therefore, when examining the content of the Report, the members of the Whistleblowing Committee will not know the identity of the Whistleblower, which is tracked in a separate database and may only be disclosed for the reasons laid down within the applicable legislation.

At the end of the reporting process:

- in the event of an anonymous report, the Digital Whistleblowing System confirms the receipt of and taking charge of the report and provides the unique identification code of the report, through

which the Whistleblower will be able to access the Digital Whistleblowing System to check any requests for clarifications and the status of the report management workflow. This code does not allow the Whistleblower to be identified in any way. It is the duty of each Whistleblower to diligently keep the unique identification code of the report, not to disclose it to others and not to allow Third Parties to access the information in the report;

- in the event of a confidential report, the Whistleblower may verify the status of the report and any requests for additions/clarifications by accessing the relevant section on the system using his/her credentials.

It is recommended that the Whistleblower periodically accesses the Digital Whistleblowing System to check for any requests for clarifications relating to the submitted report. In this regard, it should be noted that any requests for additions/clarifications will be sent to the Whistleblower by and no later than 20 working days from the filing of the report through the Digital Whistleblowing System.

5.3 Management and preliminary evaluation

Once the report has been received, the Digital Whistleblowing System gives notification of the receipt of a new report (without providing information regarding the content of the report) to the e-mail address of the Whistleblower Protection Officer. In the case of a report received through alternative channels, the Whistleblower Protection Officer will enter the report into the Digital Whistlebolwing System.

Upon receipt of a report (both through the Digital Whistleblowing System and through alternative channels), the Whistleblower Protection Officer carries out a preliminary evaluation and classifies the report, based on the relevant company of the Group and the subject-matter of the report.

In this phase the Whistleblower Protection Officer must first check whether the report is accompanied by sufficient information to assess whether it is well-founded; if the report is too general and devoid of sufficient information, the Whistleblower Protection Officer will contact the Whistleblower (through the channel used by the Whistleblower, if applicable) to obtain additional information and the necessary clarifications.

The Whistleblower Protection Officer can file the reports that are clearly unfounded, instrumental or outside the scope of this Policy. These reports are also saved in the computerized archive of the Digital Whistleblowing System, which does not allow any form of cancellation and/or alteration, unless otherwise provided for by applicable local regulations (see section 6).

It should be noted that reports that do not fall within the scope of this Policy will not be considered for the purpose of any investigation by the Whistleblowing Committee and will be sent, where appropriate, to other corporate bodies/departments, that may be competent in relation to the subject matter of the same.

Conversely, if a report is not found to be manifestly unfounded, is supported by sufficient information to assess its content, and concerns a reportable conduct as defined in section 2, the Whistleblower Protection Officer submits the report to the Whistleblowing Committee to proceed with the investigation stage referred to in the following section.

The Whistleblowing Committee may ask for support from the local departments when their specific skills and abilities are required to carry out the preliminary evaluation.

If situations of potential conflicts of interest arise during the preliminary evaluation stage, the management of the report should be entrusted only to persons who are not in conflict situations; if the conflict of interest concerns one or more members of the Whistleblowing Committee, they must refrain

from taking part in all management activities and must be replaced by others who have no conflicts of interest, identified by the other members of the Committee.

The phase of preliminary evaluation must be completed as quickly as possible, taking into consideration the possible necessity of acquiring information and clarifications, and in any event within 40 working days of the date the report is received.

5.4 Investigations and final provisions

If the report - even if not clearly unfounded, instrumental or outside the scope of this Policy - is not sufficiently detailed, the Committee formulates (through the channel used by the Whistleblower, if applicable) the appropriate requests for additions/clarifications to the Whistleblower.

Such requests for additions/clarifications will be sent to the whistleblower by and no later than 20 working days from the communication of the report.

Once the clarifications deemed appropriate have been obtained, the Whistleblowing Committee proceeds:

- with the filing of reports which are believed to be unfounded and/or not adequately documented, despite the clarifications obtained;

or

- with the investigation phase, for reports reasonably founded and supported by sufficient elements to proceed with the preliminary investigation phase.

In the latter case, the Whistleblowing Committee defines a specific "investigation plan", which identifies:

a) the methods for carrying out the investigation (requests for additions/clarifications to the Whistleblower, carrying out the checks deemed necessary, etc.);
b) the Group's companies and/or corporate departments potentially competent with respect to the matter; and
c) the timeframes within which to conclude the investigation.

Investigations may be performed, as the Whistleblowing Committee sees fit, with the support of departments, employees or Third Parties that, in relation to the content of the report, own the greatest degree of knowledge and competences to analyze the issue. The Whistleblowing Committee can take advantage of the specific skills and competences of local departments to conduct the appropriate investigations as well as establish working teams dedicated to investigating specific reports. In this context, confidentiality must be guaranteed at all times to the extent possible under local law and in order for Amplifon to be able to investigate a report and take appropriate steps.

If investigations are outsourced to an external service provider, the Whistleblowing Committee must ensure that such provider is bound by non-disclosure undertakings regarding the investigation and the information to which access is granted. The departments, employees or Third Parties involved in the "investigation plan" must guarantee full collaboration to the Whistleblowing Committee as far as necessary for carrying out the investigation, in compliance with the principles and guarantees provided for by this Policy.

At the end of the investigation phase, the Whistleblowing Committee prepares a report with its final assessment and decision (e.g., storage or adoption of further measures) and identify the corrective actions to manage the case reported and prevent new cases, including any disciplinary measures. In any case, Amplifon structures investigations to maximize its ability to claim any applicable privilege or protection over the report, according to provisions set forth by applicable local laws.

This report is then sent to the relevant corporate bodies and departments (of Amplifon and/or other companies belonging to the Group that may be involved in the report) to be implemented. The Whistleblowing Committee will ensure that any disciplinary or remedial actions resulting from the investigation are implemented, verifying their effective application.

In any case, the investigation phase concludes within 40/60 working days from receipt of the report according to its nature, except in cases where reports relating to particularly complex situations require longer evaluation times, in compliance with the principles of impartiality, competence and professional diligence, and in compliance with the duration requirements specified by local law.

5.5 Reporting activities

Every six months (or immediately in cases of urgency) the Whistleblowing Committee prepare a summary of the activities carried out regarding all the received reports (including the ones that have been filed without analysis) and sends it to the Control, Risk and Sustainability Committee.

The latter Committee ensures the monitoring of the implementation of any corrective measures defined by the Whistleblowing Committee.

5.6 Feedback to Whistleblowers

Amplifon ensures that Whistleblowers are informed and kept up to date on the process for handling the report made.

To this end, for each report made, the Whistleblower, in relation to and consistent with the reporting channel used, receives information regarding the receipt and acceptance of the report and the conclusion of the investigation.

5.7 Disclosure to the party against whom the report was made

In all report management stages, the Whistleblowing Committee evaluates whether it is possible to inform the subject of the report that a report has been submitted against him/her, that proceedings are underway and what the outcome of these proceedings is. In particular, the moment in time when the reported subject is informed of the report will be assessed on a case-by-case basis, after first checking whether disclosing this information could affect the investigations needed in order to assess the submitted report or whether involving the subject of the report is necessary for the investigation.

5.8 Disciplinary Measures

Disciplinary measures may be taken as a result of misconduct emerged from the investigation process, following a report or when a misuse of the Whistleblowing Policy is detected. The Whistleblowing Committee is entitled to recommend to the legal representatives of the relevant company of the Group the adoption of the internal disciplinary measures deemed appropriate (which may result also in the dismissal of the individual concerned) and to initiate legal proceedings.

The disciplinary measures must be appropriate and proportionate to the ascertained violation, also taking into account the criminal relevance of the conduct and the fact that criminal proceedings may be brought if the conduct constitutes a crime. The disciplinary measures must also be taken in accordance with the national collective work contracts or other national applicable provisions.

6 Tracking of the report management process

The Whistleblowing Committee ensures that all of the reports received (including the ones that have been filed without analysis) are stored in a dedicated electronic archive and that the documents relating to the reports are handled in accordance with the applicable personal data protection regulations.

All company departments involved in the report management process - within their respective competence - ensure the traceability of information. The members of the Whistleblowing Committee will be in charge of filing the received documentation relating to the reports in the dedicated electronic archive.

This documentation must be kept for at least 10 years, unless otherwise provided for by applicable local regulations.

7 Communication and training

This Policy is intended for the widest communication. To this end, this Policy:

- is sent to every company of the Group;
- is made known to Amplifon's people through adequate communication systems defined by the corporate/local HR department; and
- is published on the company intranet.

For the abovementioned purposes, each company of the Group must translate this Policy into the local language to allow for a better communication and understanding of the document.

The training for all recipients of this Policy includes specific training activities, regularly conducted and as needed.

8 Privacy

Amplifon S.p.A. hereby states that the personal data of Whistleblowers and of any other parties involved that is obtained while handling the reports will be processed in full compliance with the provisions of current legislation regarding the protection of personal data, and in any case in line with the provisions of the Privacy Organizational Model.

Only the data strictly necessary for verifying the validity of the report and for handling it will be processed. Amplifon S.p.A. will process the personal data for the sole purpose of performing the procedures set out in this Policy, without prejudice to any specific local legislation on the subject.

Under Article 4, subsection 7, of the GDPR, the Data Controller of the personal data acquired in the management of reports is Amplifon S.p.A.. With respect to any potential data transfer to non-EU Countries, Amplifon will act in accordance with applicable law.

The external Data Processor is the external supplier who manages the personal data of people involved in the reports.

Amplifon guarantees the lawful and fair processing of all personal data in compliance with applicable laws.

The text of the privacy notice concerning the processing of personal data relating to whistleblower's reports is attached to this Policy (Annex 1).

9 Support and assistance

For any questions, concerns or need for support regarding this Policy, Amplifon's people may contact the Group Internal Audit and Risk Management Officer or the Chief Legal Officer or the Chief HR Officer, who are available to provide all necessary support.

10 Controls and monitoring

The Group Internal Audit and Risk Management Officer will monitor the implementation of this Policy by the Group's companies, also through specific internal auditing activities based on the Group's Internal Audit Plan.

The Group Internal Audit and Risk Management Officer will review this Policy on a periodic basis to ensure that it remains as effective as possible, also on the basis of any observations received, new regulations and organizational changes.

11 Conclusion

PLEASE SPEAK UP

If you have any evidence or justified concerns about relevant breaches and unlawful conduct according to this Policy, please speak up!

Because it is the right thing to do, for you, for us, for everyone.

ASK FOR HELP

When seeking support and clarification, please contact:

- Group Legal Department.
- Group HR Department.
- Group Internal Audit and Risk Management Department.

DO'S AND DON'TS

DO'S	DON'TS
▪ Do not hesitate. To maintain transparent conduct, Amplifon trusts in your voice: make your voice heard	▪ Don't use Whistleblowing channels improperly, reporting personal complaints or rumored violations, without evidence, in a malicious or vexatious way
▪ Use Whistleblowing channels where you have evidence of violations	▪ Don't try to investigate the matter on your own
▪ Be specific when describing known violations	▪ Don't approach or accuse any individuals directly, but use the appropriate reporting channels

PRIVACY NOTICE CONCERNING THE PERSONAL DATA PROCESSING

- Regulation EU 2016/679-

Kind User,

in accordance with the regulations on the protection of personal data (Legislative Decree no. 196/2003 and EU Regulation no. 2016/679), Amplifon S.p.A. invites you to read the following information, which is intended to support you in understanding how Amplifon processes your personal data.

1. Processing of personal data

"Amplifon receives and processes your personal data with respect and utmost care"

The personal data provided will be processed by Amplifon in the manner of, and in compliance with, current legislation, using methods that are suitable for ensuring security and confidentiality.

In particular, the processing of these data will be performed:

- ✓ on paper and/or using digital support media;
- ✓ by persons authorized in the performance of these tasks, who have been suitably instructed and made aware of the constraints imposed by legislation concerning the protection of personal data;
- ✓ in such a way as to prevent or minimize the risks of destruction or loss, even accidental, of the data, unauthorized access or processing that is not permitted or that does not comply with the purposes of collecting the data;

The data will be processed by the Amplifon S.p.A. Corporate Division (acting as Data Controller) and possibly by the company involved and operating in the country / sector to which the Report refers.

2. Purpose of the Data processing

"We require your personal data in order to handle the Reports correctly"

Your personal data will be processed for purposes of a **mandatory** nature in relation to the correct management of Reports, in accordance with this Policy. The Data Controller collects the personal data you provide when making detailed Reports concerning:

a. unlawful conduct or violations of the organization and management models of the Company of which you have become aware within the employment relationship in accordance with the law (Law 30 November 2017, No. 179);

b. unethical conduct, contrary to the ethical principles of the Amplifon Group, in order to verify and guarantee the correct and complete application of Company Policies and to implement any activity following, and consequent to, these checks, as well as to comply with specific obligations under law, arising from the regulations and the applicable legislation with reference to precise needs relating to the Company's internal control and monitoring of business risks, as specifically required by law.

The provision of your personal data is optional; however, in the case of refusal, it will not be possible to use the whistleblowing system in order to report behavior that is contrary to applicable law as well as to the ethical principles of the Amplifon Group.

3. Legal basis of the Data processing

"Data processing is required to pursue the legitimate interest of the Data "

Your personal data may be processed without your consent, in cases where this is necessary to pursue the legitimate interest of the Data Controller in order to receive and manage the reports of actual or suspected breaches and violations of the laws and regulations applicable to Amplifon companies as well as to internal policies and procedures. The processing of the data will be enacted according to the principles of purpose, relevancy, adequacy and limitation.

4. Categories of Processed Data

"As part of the management of Reports, we may process your common and sensitive personal data"

Amplifon may process the following personal data and information provided:

a. your name and contact details (unless the Report is anonymous);

b. the name and personal data of other persons provided in the Report (e.g., description of the functions and contact information); and

c. the description of the alleged infringement, as well as a description of the circumstances of the case.

Note that depending on the laws in force in the country in which the Whistleblower is resident, reporting may not be allowed in an anonymous form; however, personal data will be processed confidentially and will only be disclosed according to the rules set out below.

Particular categories of personal data (e.g., related to race or ethnicity, health, sex life, religion or personal beliefs or union membership) could be collected as a consequence of a Report. In this case, such data will be processed only

if and when they are relevant for the purposes of reporting and only to the extent allowed by applicable law and / or the need to ascertain, exercise or defend a right in a legal claim pending before a court. If, on the other hand, these data are not relevant for the purposes of reporting and are beyond the scope permitted by applicable law and / or are not necessary in order to ascertain, exercise or defend a right in a legal claim pending before a court, then they will be deleted promptly and securely and will not be further processed.

5. Communication of personal data

"Your data will be processed only by the people specifically authorized by Amplifon"

For the purposes described in section 2 above, the personal data provided may circulate in the following areas:

A. Within Amplifon - The data may be used by Amplifon personnel who have been assigned to a specific role as data controller or processor who are committed to confidentiality and to whom appropriate instructions have been given.

Your personal data will be made accessible only to those subjects who, within the Company, require it in consideration of their job or hierarchical position. These subjects will be suitably instructed in order to avoid the loss, destruction, unauthorized access or unauthorized processing of data.

In addition, the data may be used by third companies that perform instrumental activities on behalf of the Company such as:

a. **Service providers** (including IT companies) which are entrusted with specific management of contractual obligations;
b. **Companies belonging to the same group to which Amplifon S.p.A. belongs**, for investigation purposes;
c. **External consultants** for the management of the investigation process and legal assistance, firms and companies in the context of assistance and consultancy relationships.

These companies act as external data processors and under the direction and monitoring of Amplifon.

B. Outside Amplifon (Public or controlling entities) - In addition, again for purposes strictly instrumental to the assessment of the Reports and in the implementation of legal or contractual provisions, the Company, directly or indirectly, transmits some of its personal data, according to a strict criterion of pertinence, to the following categories of persons to whom communication is strictly necessary for the management of the employment relationship:

a. public security authorities;

b. judicial authorities.

These entities will act as independent Data Controllers of the respective processing operations, unless they act on behalf of Amplifon as external Data Processors and have therefore signed a specific contract governing the processing entrusted to them, pursuant to art. 28 of GDPR.

6. Communication of your personal data to third parties

"Your data will never be made available to unidentified subjects"

In compliance with the GDPR, your personal data obtained from time to time may be used to update and correct the previously collected information.

Personal data are accessible to the Data Controller's personnel, duly authorized on the basis of necessity criteria, and communicated to third parties in the following cases:

a. when disclosure is required by applicable law and regulations with respect to legitimate third parties, such as authorities and public bodies for their respective institutional purposes (e.g., anti-money laundering legislation, judicial authorities);

b. disclosure to third parties in the case of extraordinary transactions (e.g., mergers, acquisitions, sale of companies, etc.).

Your data may also be disclosed to third-party suppliers who support us in providing the services necessary for managing the Reports, duly appointed as data controllers in accordance with the provisions of the GDPR.

Finally, for the purposes set out above, Amplifon Group companies may access your personal data, as independent Data Controllers, if the Reports concern Amplifon Group's employees.

7. Retention of personal data

"Your data will be kept for as long as we consider necessary for the management of the Report"

Your personal data will be processed and stored by the Data Controller, in line with Amplifon's Data Retention Policy, for the time necessary to manage the Reports and for the period of time strictly necessary in order to fulfil the purposes for which they were collected and for the fulfillment of applicable legal obligations.

Moreover, the data shall be deleted or lastingly anonymized when the above aims are achieved, unless the Data Controller is required to keep the Data for a further period of time in order to comply with legal obligations.

In any case, your data will not be kept for more than 10 years from the submission of the Report.

We also inform you that, pursuant to Articles 5 and 89.1 of the GDPR, for statistical purposes only, your personal data may be kept anonymously for periods of time that are longer than those specified in the previous paragraph, without prejudice to the implementation of those appropriate technical and organizational measures required in order to protect your rights and freedoms.

8. Transfer of personal data outside the EU

"Your data might be transferred outside the European Union, but we guarantee you an adequate level of protection"

Some of the Amplifon Group Companies that receive your personal data are also established outside the European Union, in countries that do not guarantee an adequate level of personal data protection under the GDPR. The Data Controller will take the necessary legitimate data transfer precautions (e.g., through the implementation of the Standard Contractual Clauses approved by the European Commission).

9. Rights of the data subject

"You have the right to request access, rectification, portability and cancellation of your data, as well as the restriction and objection to processing"

In relation to the processing of your personal data, you have the right to obtain from the Data Controller:

- ✓ **Access**: confirmation as to whether or not your personal data are being processed, and, where that is the case, access to the personal data as well as clarifications in relation to the present Privacy notice;
- ✓ **Rectification**: rectification of inaccurate or incomplete personal data;
- ✓ **Cancellation**: erasure of personal data when they are no longer necessary in relation to the purpose, when they are unlawfully processed, when they have to be erased in compliance with a legal obligation, and in the case of objection to the processing;
- ✓ **Restriction**: restriction of processing where one of the following applies:
  - If contesting the accuracy of the personal data for a period enabling the Data Controller to verify the accuracy of the personal data;
  - If opposing the erasure of the personal data in the case of unlawful processing;
  - the controller no longer needs the personal data for the purposes of processing, but they are required by you for the establishment, exercise or defense of legal claims ;
  - you have objected to the processing pending the verification whether the legitimate grounds of the controller override those of the data subject.
- ✓ **Objection:** objecting at any time to the processing of your personal data, unless Amplifon demonstrates compelling legitimate grounds for the processing which override your interests, rights and freedoms (e.g., the establishment, exercise or defense of legal claims);
- ✓ **Portability**: obtaining your personal data which you have provided to the Data Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller.

Moreover, we inform you that you have the right to file a complaint to the competent Control Authority.

At any time, you may request the exercising of the above-mentioned rights from Amplifon S.p.A. in sending your request to the following email address: privacygroup@amplifon.com.

10. Data Controller, Data Manager and DPO

"The Data Controller of your personal data is Amplifon. The list of Data Managers is available at your request. The DPO is the Chief Legal Officer"

- The Data Controller is Amplifon S.p.A. Corporate Division, registered office in via Ripamonti n. 133, 20141 Milano, in the person of its *Chief Executive Officer pro-tempore* ("**Data Controller**");
- The updated list of the Data Processors appointed can be requested at: privacygroup@amplifon.com;
- You can contact the Group Data Protection Officer ("**DPO**"), in the person of its *Chief Legal Officer pro-tempore,* at any time at the following email address: privacygroup@amplifon.com.


amplifon