Group
Whistleblowing Policy

Amplifon S.p.A.

Contents

1 Introduction

Why a Whistleblowing Policy

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

For this reason, Amplifon encourages and highly recommends raising concerns about the breach of these principles and takes extremely seriously any possible whistleblowing report as identified in this Policy. *(Please refer to the dedicate section "2. What to report").*

To this end, we have implemented within the Group the Whistleblowing System described in this Policy, which is designed based on the highest international standards that relies on the best available digital technologies.

Through this system, we guarantee that the confidentiality of your reports will be protected to the extent possible under applicable law. We also guarantee that no Amplifon people will be dismissed, demoted, suspended, threatened, harassed, retaliated against, or discriminated in any way in their working conditions for submitting a report in accordance to this Policy.

Similarly, no Amplifon people will be adversely affected by reporting possible violations which could be found to be unsubstantiated if there was a reasonable belief to justify reporting them.

Whistleblowing Policy applicability

This document contains rights and obligations concerning Whistleblowers and the Whistleblowing reporting process and applies to all Amplifon companies in all geographies 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.

The specific aspects relating to each country's laws are reflected in the different boxes in the present document and will be transposed into the setting of the Digital Whistleblowing System, if needed. All the addressees of this Policy are therefore invited to examine the annexes to identify those for which they are responsible.

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 Amplifon Group operate, or the obligations to submit reports to any control bodies established at each Group company.

This Policy has been approved by the Board of Director of Amplifon S.p.A. on 4 March 2020 and its application is mandatory for all the Amplifon companies.

Each Amplifon company will adopt this Policy (and any new version of the same) through a resolution of its Board of Directors (or of the corresponding body / function / role if the governance of the respective company does not provide for such body) promptly during the first useful meeting

and in any case no later than 60 working days from the formal communication date from the Amplifon CEO consistently with the implementation plan.

The companies that should be established and / or join the Amplifon Group after the approval of this Policy will adopt the same through the resolution of their Board of Directors (or of the corresponding body / function / role if the governance of the respective subsidiary does not provide for this body) promptly during the first useful meeting and in any case no later than 60 working days from the date of incorporation or, as appropriate, from joining the Amplifon Group.

When required by local legislations, the relevant Amplifon company ensures that this Policy (and any new version of the same) will be duly submitted to the authorization or approval of the competent authorities or councils.

2 What to report

The Whistleblowing channels serve the purpose of reporting actual or suspected breaches and violations of which Amplifon people or Third Parties become aware or of which they have reasonable suspicion concerning conduct (of any nature whatsoever, even if merely omissive) in violation of:

(i) the Group Code of Ethics;
(ii) the laws applicable to each Amplifon companies, including (but not limited to) the anti-corruption laws;
(iii) regulations or measures issued by any competent Authority; and/ or
(iv) internal policies and procedures adopted by the Amplifon companies (specifically, policy concerning conflicts of interest, anti-corruption, Model 231 for Amplifon S.p.A.).

The foregoing, without prejudice to different provisions under applicable local legislation, is transposed in the settings of the Digital Whistleblowing System.

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. We recommend speaking with the people mentioned under following Section 9 if you are not sure whether secrecy or privilege laws or regulations apply to a planned report.

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, excluding final customers, with whom the Amplifon company has some form of business relationship (e.g. joint ventures, joint venture partners, consortium partners, outsourcing providers, contractors, consultants, sub-contractors, suppliers, vendors, advisors, agents, distributors, representatives, intermediaries and investors).

Reports shall be made based on a reasonable belief and as detailed as possible. The concerns shall contain information and facts rather than allegations or statement of opinions, without prejudice to any specific additional requirement provided by applicable local laws.

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

WHAT TO REPORT – IN AUSTRALIA

Disclosures may be made about misconduct or an improper state of affairs or circumstances in relation to Amplifon Australia (including by an Amplifon Australia current or former officer or employee) where you have reasonable grounds to suspect has occurred or is occurring in relation

to Amplifon Australia. A discloser may wish to obtain independent legal advice before making a disclosure.

Disclosures **solely** about a personal work-related grievance are **not** covered by this policy and do **not** qualify for protection under the Australian whistleblower laws unless they also relate to any detriment or threat of detriment by reason of you making or being suspected of making a protected disclosure. In particular, - as a further specification to the matters set out in Section 2 of the Global Whistleblower Policy- disclosures about the following matters may qualify for protection under the Australian whistleblower laws:

I conduct that amounts to a criminal offence or contravention of the *Corporations Act 2001* (Cth) or *Australian Securities and Investments Commission Act 2001* (Cth);

II conduct that is a Commonwealth criminal offence punishable by more than 12 months imprisonment;

III illegal conduct, such as theft, dealing in, or use of, illicit drugs, actual or threatened violence, corruption, bribery, criminal damage to property or breaches of work health and safety laws;

IV fraud, money laundering or misappropriation of funds;

V negligence, default, breach of trust or breach of duty;

VI any conduct that may indicate a systemic issue in relation to Amplifon Australia;

VII product liability;

VIII conduct relating to business behaviours and practices that may cause consumer harm;

IX conduct that represents a danger to the public or the financial system;

X information that indicates a significant risk to public safety or the stability of, or confidence in, the financial system;

XI misconduct in relation to Amplifon Australia's tax affairs; or

XII engaging in or threatening to engage in detrimental conduct against a person who has made a disclosure or is believed or suspected to have made, or be planning to make, a disclosure.

3 Roles and Responsibilities

- **Whistleblower Protection Officer**: the Group Risk and Compliance Officer, which is responsible for receiving, collecting and preliminarily analyzing reports submitted by Whistleblowers and calling for the Whistleblowing Committee meeting.
- **Whistleblowing Committee:** the committee appointed by the Board of Directors of Amplifon S.p.A. and composed by (i) the Group Risk and Compliance Officer, (ii) the Chief HR Officer and (iii) the Chief Legal Officer, designated to investigate, record and report to the Control, Risk and Sustainability Committee concerns issued through Whistleblowing channels and to define the related disciplinary measures.
- "**Whistleblowers**" responsible for submitting Whistleblowing reports: as the case may be, Amplifon directors, officers, managers, employees as well as the Third Parties.

ROLES AND RESPONSIBILITIES – IN AUSTRALIA

In addition to the individuals identified in Section 3 of the Group Whistleblower Policy, eligible whistleblowers in Australia include current or former:

I officer or employees of Amplifon Australia;

II supplier of goods and services to Amplifon Australia;

III an associate of Amplifon Australia;

IV parent, grandparent, child, grandchild, sibling, spouse or dependent of any of the above.

Disclosures that qualify for protection may be made to any of the people listed below. However we encourage disclosures under this policy to be made on the Amplifon Digital Whistleblowing System available here: (*https://whistleblowing.amplifon.com*). This is an independent, confidential, anonymous and secure platform where a discloser may track the progress of their disclosure – the anonymity of reports made on this platform will be retained even after the investigation into the disclosure is finalized.

In addition to the individuals identified in Section 3 and 5.1 of the Group Whistleblower Policy, a disclosure may be made to any of the following eligible recipients:

I the Amplifon Whistleblower Protection Officer;

II Amplifon Australia officers and senior managers;

III internal or external auditor of Amplifon Australia; and

IV any employee or officer who has functions or duties relating to the tax affairs of Amplifon Australia.

DISCLOSURES TO EXTERNAL PARTIES – IN AUSTRALIA

The protections afforded by the Australian whistleblower laws (set out in section 5 below) also include some types of disclosure made to external parties, such as:

V legal representatives, to obtain advice or representation about the Australian whistleblower laws;

VI Australian Securities Investment Commission (**ASIC**), Australian Prudential Regulatory Authority (**APRA**) or the Australian Taxation Office (**ATO**); or

VII MPs or journalists, where you have reasonable grounds to believe that making the further disclosure would be in the public interest or the information concerns a substantial and imminent danger to the health or safety to one or more persons or to the natural environment, but **only if**:

a. you previously made a disclosure of that information to either ASIC, APRA or another Commonwealth body prescribed by regulation; and

b. you notified that body in writing of your intention to disclose to an MP or journalist (where, for public interest disclosures, **at least 90 days** must first have passed since your previous disclosure before this notice may be given).

Strict criteria apply and independent legal advice should be obtained before making a disclosure to an MP or journalist. For more information about the Australian whistleblower laws (including how to make a disclosure directly to ASIC or the ATO), see the information available on the ASIC website (including Information Sheet 239 How ASIC handles whistleblower reports and Information Sheet 247 Company officer obligations under the whistleblower protection provisions) and the ATO website.

The above-mentioned external parties should, as far as is reasonably practicable, transmit the disclosure to Amplifon through the Amplifon Digital Whistleblowing System available at https://whistleblowing.amplifon.com).

Please be aware that disclosures made directly to the external parties may not guarantee the same confidentiality and timeliness ensured with respect to reports submitted through the Amplifon Digital Whistleblowing System.

4 General principles

4.1 Confidentiality

All reports shall 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 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 the same 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 are adopted:

- the transmission/storage of the reported information is carried out through the Whistleblowing System; if exceptionally submitted through means other than the Whistleblowing System, the reports must be promptly loaded into the 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 management process of the whistleblowers' reports are carried out in a protected electronic environment, accessible only to specifically authorized persons, 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 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 by the applicable legislation.

CONFIDENTIALITY – IN AUSTRALIA

In addition to the matters set out in Section 4 of the Global Whistleblower Policy above:

I a Whistleblower's identity will not be disclosed without their consent unless an exception applies under law;

II there is no obligation on the Whistleblower to maintain confidentiality of the disclosure; and

III disclosures made anonymously are protected under Australian law. Anonymous reports will remain anonymous after an investigation is finalized, including in internal reporting.

4.2 Non-retaliation

No Whistleblowers reporting a breach based on a reasonable belief in accordance with the provisions of the present procedure 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 particular, no Amplifon people can be dismissed, demoted, suspended, threatened, harassed or discriminated in any way in their working conditions for having submitted reports in compliance with 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 in 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 punished. To implement this principle a Whistleblower protection programme has been put in place to protect Whistleblower from any form of retaliation.

This protection programme is based on the direct and express commitment of the company's executives, in the persons of directors and top management (known as "top-level commitment"). The protection programme envisages:

- the availability of the Whistleblowing System - as well as the alternative channels indicated in section 5.1 - to report any violator of the non-retaliation principle to the Whistleblowing Committee;
- the duty of the Whistleblowing Committee to timely conduct of the related investigations is guaranteed, with the support of the functions 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 directors and the top management of the Group 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 Human Resources Function, monitors any retaliation, unfair, discriminatory behaviors towards reporting persons, through the analysis and overall assessment of specific "Red Flags" (a by way of example: changes of office or job, transfers of headquarters, requests for job changes, long absence due to illness, disciplinary challenges / measures, requests for unpaid leave, negative performance assessments, etc.).

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

All Amplifon 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 Amplifon 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 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.

MISUSE OF THE WHISTLEBLOWING POLICY – IN AUSTRALIA

You may still qualify for protection even if your disclosure is found to be incorrect or defamatory but you must have reasonable grounds for suspecting that the information you are disclosing concerns misconduct or an improper state of affairs or circumstances in relation to Amplifon Australia (see Section [2] above). A disclosure made without reasonable grounds (such as where you know it to be false) may amount to misconduct and subject to disciplinary action by Amplifon Australia.

4.5 Duty of independence and professionalism in the management of reports

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

4.6 Protection of the integrity of reports

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

4.7 Other remedies

A whistleblower will be protected from any civil, criminal or administrative liability in relation to their disclosure in compliance with applicable local law provisions. Applicable compensation provisions shall also apply.

PROTECTIONS – IN AUSTRALIA

Amplifon Australia is legally required to comply with the protections provided by the Australian whistleblower laws:

I individuals are also protected from suffering harm (such as physical damage, damage to reputation or psychological harm) by reason that they are a whistleblower, suspected of being a whistleblower or propose to be a whistleblower; and

II Amplifon will ensure fair treatment for any employee/s who make or who are mentioned in protected disclosures. Amplifon Australia has in place processes for protecting, supporting and monitoring the welfare of these employees. This includes risk assessment of any potential detriment, work adjustment considerations and support services such as counselling.

Whistleblowers (or any other employee or person) can seek compensation and other remedies through the courts if they suffer loss, damage or injury because of a disclosure and Amplifon Australia failed to take reasonable precautions and exercise due diligence to prevent the detrimental conduct.

5 Process Management

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

5.1 Whistleblowing channels

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

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 – Italia

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 reporting parties 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/express courier avoiding any email or digital forwarding to the Whistleblower Protection Officer who shall take care to 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 web link of the Digital Whistleblowing System: the Whistleblower will be directed to a first screen that allows to (i) submit a report or (i) check the status of a previous report.

In case the Whistleblower select the "Report" button, a second screen will open where two reporting options will appear: one for the Amplifon employees and one for the Third parties.

In case the “Employee” option is selected, the Whistleblower can choose to submit his/her report by logging in with Single Sign On (**confidential report**) or to report anonymously (**anonymous report**).

Similarly, in case 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 fields required therein).

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 Amplifon company 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 covered by the report and the persons involved (potential managers and possible witnesses), 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 and the reported person and automatically inserts them in a separate archive electronically managed by the Whistleblower Committee and accessible only to the members of this Committee. Therefore, when examining the content of the Report, the members of the Whistleblowing Committee will not be allowed to know the identity of the Whistleblower, which is tracked in a separate database and may only be disclosed for the reasons laid down in the applicable legislation.

The Digital Whistleblowing System then displays an initial information confirming receipt 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 recommended that the Whistleblower periodically access 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 no later than 20 working days from the filing of the report through the Digital Whistleblowing System.

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 on the report.

5.3 Handling over and preliminary evaluation

Once the report has been received, the Digital Whistleblowing System notifies 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.

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 Amplifon company 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 its well-foundedness; if the report is too general and devoid of sufficient information, the Whistleblower Protection Officer will contact the Whistleblower through the Digital Whistleblowing System to obtain additional information and the necessary clarifications.

The Whistleblower Protection Officer can ignore and not manage ("discard") the reports that are clearly unfounded, instrumental or outside the scope of this Policy. Even the "discarded" reports are 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 in applicable local regulations (see section 6).

It should be noted that reports that do not fall within the scope of this Policy will be considered as not received and therefore will not be taken into consideration or sent to other corporate bodies / functions 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 submit 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 to the local functions when their specific skills and abilities are required to carry out the preliminary evaluation.

If situations of potential conflicts of interest arise in 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 Investigation and final decision

Reports that have not been immediately "discarded" are submitted to the assessment by the Whistleblowing Committee.

If the report - although not clearly unfounded, instrumental or outside the scope of this Policy - is not sufficiently detailed, the Committee formulates (through the Digital Whistleblowing System) the appropriate requests for additions / clarifications to the Whistleblower.

Such requests for additions / clarifications will be sent to the whistleblower no later than 20 working days from the communication of the report through the Digital Whistleblowing System.

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

– with the filing of reports which are without foundation 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 possible Group companies and / or corporate functions competent with respect to the matter; and
c) the timeframe within which to conclude the investigation.

Investigations may be performed, as the Whistleblowing Committee sees fit, with the support of functions, employees or Third Parties that, in relation to the report's content, 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 functions to conduct the appropriate investigations as well as establish working teams dedicated to investigating specific reports. In this context, confidentiality shall be granted at all times to the extent possible under local law and in order for Amplifon to investigate a report and take appropriate steps.

If investigations are outsourced to an external service provider, the Whistleblowing Committee shall ensure that such provider is bound by non-disclosure undertakings regarding the investigation

and the information to which access is granted. The functions, 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 written report with its final assessment and decision (e.g., storage or adoption of further measures) and identify the corrective actions to manage the issues reported and prevent new issues, including any disciplinary measure. 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 functions (of Amplifon and/or other company belonging to the Amplifon Group that may be involved in the report, as the case may be) to be implemented. Whistleblowing Committee will ensure that any disciplinary or remedial actions resulting from the investigation are implemented. When disciplinary actions are defined, the Whistleblowing Committee shall assure that they are effectively executed collecting related evidence.

In any case, the investigation phase is completed within 40 working days from the receipt of the report - except in cases where reports relating to situations of particular complexity require longer evaluation times and, in any case, not exceeding 60 working days - in compliance with the principles of impartiality, competence and professional diligence. Complex investigations may take longer, and they will be conducted in compliance with any duration requirements specified by local law.

INVESTIGATIONS PROCESS MANAGEMENT – IN AUSTRALIA

The following steps will typically be taken for investigations of disclosures made in Australia and clauses 5.1 – 5.4 of the Amplifon Group Whistleblowing Policy will be applied only if they are compatible with the provisions below. This process may vary depending on the nature of the disclosure.

I The Amplifon recipient listed in Section 3 above will direct the discloser to the Amplifon Digital Whistleblowing System available here: (https://whistleblowing.amplifon.com) which will notify the Whistleblower Protection Officer [(or the Whistleblowing Committee if the disclosure is about the Whistleblower Protection Officer)]. If the discloser does not wish to use the Digital Whistleblowing System, the Amplifon recipient will use the Digital Whistleblowing System to log the disclosure as soon as practicable removing any information which may identify the discloser (unless consent has been provided to reveal their identity).

II The Whistleblower Protection Officer (or the Whistleblowing Committee) will share the disclosure reference number with the discloser through the Digital Whistleblowing System and invite the discloser to use the Digital Whistleblowing System or to contact the Whistleblower Protection Officer (or the Whistleblowing Committee) for updates.

III As soon as practicable, the Whistleblower Protection Officer addresses the Whistleblowing Committee to (or the Whistleblowing Committee itself must) determine whether the disclosure falls within the scope of the Australian whistleblower laws and, if so, whether a formal, in depth investigation is required.

IV	If an investigation is required, the Whistleblowing Committee must: a. determine whether the investigation of the disclosure should be conducted internally or externally; b. in if the Whistleblowing Committee determines that the investigation should be conducted internally, appoint an investigator (or a team, as the case may be) with no personal interest in the matter to conduct an internal investigation into the matters disclosed (if they determine it to be necessary or appropriate); c. if the Whistleblowing Committee determine that the investigation should be conducted externally (to ensure fairness and independence or because specialist skills are required), they will refer the disclosure to a nominated external agency, who will then conduct an investigation into the matters disclosed; The investigator must conduct any investigation in an objective and fair manner, ensuring to provide any individual who has been adversely mentioned in information provided by a Whistleblower an opportunity to respond to the allegations made in respect of them prior to any adverse findings being made;
V	All contact with the discloser in the investigation of the disclosure must be, where appropriate, documented in the Amplifon Digital Whistleblowing System bearing in mind confidentiality and identity protection requirements.

5.5 Reporting

Every six months (or immediately in case of urgency) the Whistleblowing Committee draws up a summary of all activities carried out regarding all the received reports (including the ones that have been "discarded") 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. The Whistleblowing Committee receives the results of this monitoring every six months.

5.6 Feedback to Whistleblowers

Amplifon ensures Whistleblowers to be informed and kept duly updated about the management process of the report during each phase of the investigation process.

To this end each whistleblower, with respect to and consistently with the whistleblowing channels used, receives an initial confirmation that the report has been received and is being dealt with and a final information that the investigation has been closed; furthermore, the Whistleblower may access the Digital Whistleblowing System at any time to check the status of his/her report(s) using the assigned personal code.

5.7 Disclosure to the party against whom the report was made

In all management stages of the reports, the Whistleblowing Committee evaluates whether it is advisable 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. More specifically, the time when the party against whom the report was made will be 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 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 Whistleblower's 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 Amplifon company the adoption of the internal disciplinary measures deemed appropriate (which may result 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 adopted measures must also be taken in accordance with the national collective labor agreements or other national applicable provisions.

6 Tracking of the report management process

The Whistleblowing Committee ensures that all the reports received (including the ones that have been "discarded") are stored in a dedicated electronic archive and that the documents relating to the reports are handled in accordance with the legislation for the management of information classified as "confidential" in accordance with applicable data protection regulation.

All company functions 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 archiving 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 in applicable local regulations.

7 Communication

This Policy has the widest communication. To this end, this Policy:

- is sent by the Group CEO to each of each Amplifon company;
- is made known to Amplifon people by being posted in the spaces dedicated to corporate communications; and
- is published on the corporate intranet and on the Group website.

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

The Human Resources function shall, to the extent applicable, ensure that new employees receive a copy of this Policy at the time of recruitment.

Training on this Policy is part of the training process for all the recipients of the same and is carried out on a regular basis, 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 GDPR, the Data Controller of the personal data acquired in the management of reports is Amplifon S.p.A. – Corporate Division. With respect to any potential data transfer to non-EU Countries or from non-EU countries to EU countries, Amplifon will act according with applicable local law.

The external Data Processor is the external supplier who manages personal data's 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 8).

9 Support and assistance

For any questions, concerns or advice regarding this Policy, Amplifon people should always contact:

(i) the Group Compliance & Risk Officer: [insert contact details],

(ii) the Chief Legal Officer: [insert contact details], or

(iii) the Chief HR Officer: [insert contact details],

which are available to provide all necessary support.

10 Controls and monitoring

The Group Compliance & Risk Officer will monitor the adoption of this Policy by the Amplifon companies; the Chief HR Officer will oversee the training of Amplifon people.

Amplifon Group's Internal Audit will independently examine and assess the internal control system to verify whether the provisions of this Policy are complied with, based on its annual audit program.

The Group Compliance & Risk Officer must periodically review this Policy to ensure that it maintains the greatest possible efficiency. Furthermore, the business units, the Internal Audit and the external auditors must indicate any possible gap in or critical issue arising from this Policy. If a violation is detected, the Group Compliance & Risk Officer will evaluate whether a review of this Policy would help to prevent the violation from recurring.

11 Conclusion

PLEASE SPEAK UP

If having concerns about breaches and violations relevant according to this Policy please speak up.

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

ASK FOR ADVICE

When seeking for advice, please contact:

- Group Risk & Compliance Function.
- Group Legal Function.
- Group HR Function.

DO'S AND DON'TS

DO'S

- Do not hesitate. Amplifon trusts in transparent conduct through your voice: speak up
- Use Whistleblowing channels where you have evidence of violations
- Be specific when describing known violations

DON'TS

- Don't use Whistleblowing channels improperly, reporting personal complaints or rumored violations, without evidence in a malicious or vexatious way
- Don't try to investigate the matter on your own
- Don't approach or accuse any individuals directly, but use the appropriate reporting channels